SECTION C

Biometrics for Authentication/Monitoring Academic Integrity: Surveying ERAU-W Student Acceptance and Insights

David D. Hernandez

Embry-Riddle Aeronautical University – Worldwide

Author Note

David D. Hernandez, College of Aeronautics, Embry-Riddle Aeronautical University – Worldwide.

The author wishes to convey special thanks to: Anne Marie Casey, Kathleen Citro, Bruce Conway, Heather Garten, Amy Jefts, Wendi Kappers, Robin Lawther, Joseph Mondello and the ERAU IT Team, Katherine Moran, Ian McAndrew, Kevin Norris, Patricia Puzzo, Jason Ruckert, Todd Smith, and Rebecca Vasquez - all of whom either shared ideas that were incorporated into the publication of this paper or assisted in obtaining student response to the survey.

Correspondence concerning their article should be sent to David Hernandez via Email: hernad17@erau.edu

ABSTRACT

A confidential survey, mirroring a previous study, was used to investigate the effect of demographic differences in ERAU-W's student body on authentication/monitoring – directly applicable to Ignite as it relates to remote modalities. Over 8,000 randomly selected ERAU-W students – both graduate and undergraduate – were invited to participate. After an introduction, with definitions and basic concepts, students answered 11 questions online. The study attempted to differentiate between student acceptance of biometrics for academic integrity as implemented by the University and the same implemented by a third party partner. Additionally, the study investigated differences in perception of video/audio-based monitoring versus non-visual sensors. The author investigated correlations between age, military status, gender, and graduate/undergraduate status, respectively, and the specific preferences expressed in the survey. The selected sample of ERAU-W’s student body exhibited negativity toward third party implementation, but not with the same intensity as the previous study. Students revealed a predilection for fingerprint-based biometrics over video/audio monitoring.

Introduction

With the topic of this year's Bollinger Rosado Teaching and Learning Effectiveness Symposium being "Research-Based Learning" and a recent focus on promoting research activities which are embedded within the courses taught in the various Embry-Riddle – Worldwide (ERAU-W) modalities, it is important to consider how this shift towards student research will be affected by the remote-learning concept that ERAU-W continues to encourage and refine. The ERAU Ignite Integration Model (Embry-Riddle Aeronautical University, 2012), which at its core is meant to create a research-supportive culture, faces unique challenges when combined with remote-learning. A critical component in promoting a research mindset, as well as expanding and enhancing the aviation-related courses offered by ERAU-W, will be the ability to provide foster an environment that supports academic integrity. This capability affects not only the perception of fairness and equity among students but also the reputation of the University and the overall validity of online course offerings. It is becoming increasingly clear in the online delivery of courses that mirroring standard, brick-and-mortar methods of maintaining academic integrity is insufficient. Stated succinctly by Semple, Hatala, Franks, and Rossi (2011),

> The reality is that some college students cheat in face-to-face classrooms; however, the potential for on-line fraud exceeds that of traditional classroom protocols. Because of reduced personal contact, on-line teaching requires additional ways to prevent cheating and to authenticate authorship of course submissions. (p. 181)

As Embry-Riddle continues to expand degree offerings, the ability to conduct laboratory work remotely via *virtual labs* currently in development and the availability of electronic textbooks and primary source materials will become increasingly important. In attempting to establish a remote undergraduate engineering program through the "2+2" initiative and, more recently, the Associate of Science in Engineering degree program, it is apparent that ABET, Inc. accreditation (ABET Engineering Accreditation Commission, 2012) is dependent on the integration of research skills - taught by engaged/versant/practicing faculty - and hands-on laboratory work into the curriculum. With such a targeted, systematic focus on both faculty and student research, intellectual property considerations will take center stage, as research leads to new discoveries and patentable methods and products. Imagine the legal questions that could arise from a working student accessing ERAU's educational resources from a shared company computer with automatic password retention, only to have those academically-licensed resources used for private company work in the development of a significant, profitable new technology. All of the discussed functions – access to laboratories, equipment, and software; access to third party research materials; and final ownership of work – depend first and foremost on the ability to accurately identify the individual with whom ERAU-W is interacting remotely and to ensure that the credential used to log on to all of our systems – currently accessible through a "single sign-on" username and password – is not being misappropriated accidentally or maliciously.

Where malicious misappropriation is concerned, in one-on-one discussions between the author and ERAU-W personnel from the full-time faculty, the Instructional Design and Development Department (IDD), the Rothwell Center for Teaching and Learning Excellence (CTLE), and the Department of Online Learning, it was repeatedly stated that the perceived increase in opportunity online, combined with the additional incentives for students to artificially inflate their performance, were of particular concern to ERAU-W. Because of the differing demographics of the Worldwide student base as compared to those of traditional universities, the temptation to participate in unethical behavior can have a different fundamental impetus. Some military personnel and business professionals, receiving tuition reimbursement in proportion to their academic performance, for example, have a financial incentive for achieving better grades that may be absent from other students.

The advent of new methods of teaching and interacting with students has similarly led to new methods of misrepresenting academic performance. One need only consult websites such as http://boostmygrades.com/ or http://essayshark.com/ to see that businesses are already profiting from the new opportunities for impropriety created by online instruction and inexpensive/instantaneous/ubiquitous communications. Similarly advanced methods and technologies will need to be employed to deter and counteract academic misrepresentation. Critical to making sound decisions in this area is a solid understanding of user perceptions and potential acceptance when it comes to two critical areas: *Authentication* – ensuring that someone is who they say they are (can be one-time or continuous); and *Academic Monitoring* – continuously reviewing user content and behaviors to ensure propriety.

While the extent of academic integrity problems in ERAU-W has not been quantified as yet, anecdotal evidence suggests that proactive steps can be taken to make improvements, irrespective of the current state. Indeed, more than one study (King, Guyette, & Piotrowski, 2009, for example) has concluded that something as simple as establishing clear, consistent statements of expected behavioral norms – a university code of ethics and standardized classroom policies, for example – is sufficient to affect students' behavior in this area. Students can take advantage of ambiguous academic policies to circumvent the intended practices or even to obstruct more stringent proctoring and oversight, siting personal privacy concerns and a lack of sufficient notification. The first step in soliciting willing cooperation from all students, faculty, and administration is to ensure that policies are clear from the outset (for students, at first enrollment in the degree program).

Regardless of ERAU-W's preferred academic integrity approach, outside influences may necessitate a different one, with varying resultant cost and complexity. In this area, foresight of the forces in play and thorough understanding of the University's available responses will become important. In the Higher Education Opportunity Act (HEOP), the U.S. Department of Education (2008) includes the statement,

> requires an institution that offers distance education or correspondence education to have processes through which the institution establishes that the student who registers in a distance education or correspondence education course or program is the same student who participates in and completes the program and receives the academic credit. (sec 496.B.ii)

With national standards evolving, ERAU-W may be required by state/national accreditation bodies or even institutions providing educational funding to utilize techniques for authentication and monitoring that go well beyond the currently-employed username and password method. In addition, legal definitions of privacy can become a factor with the array of information transactions that online institutions require in order to perform regular activities. Consider, for example, compliance with the Family Educational Rights and Privacy Act (FERPA). As McConahay and West (2012) point out:

> …conducting business online with students we never meet in person is particularly complex and challenging… Institutions offer an array of information displays and services to enable their students to conduct business from remote locations. Often, this information can be accessed only by the student to whom it pertains. Ensuring that the information is available only to intended recipients relies on sufficient assurance in the

> links among user, credential, and record. …how certain can you be when a particular physical individual says, “That digital dossier is about me”? (p. 60)

It is possible to envision a scenario where it is argued that online username and password systems, established for convenient accessibility by a remote user and initialized by a remote individual, are an insufficient safeguard against the unauthorized access of personal information.

In spite of the mounting evidence that new technology approaches to academic integrity will gain traction, multiple researchers (Cluskey, Ehlen, & Raiborn, 2011) point out that the high cost associated with deploying enhanced authentication/monitoring technologies and the unlikelihood of student acceptance of the practices calls true feasibility into question. Cluskey, et al. (2011) recommend employing several less-costly alternatives which, the authors contend, can achieve similarly beneficial results. Indeed, many of the technologies which yield the lowest risk of repudiation rely on biometrics – features of an individual that can be used to uniquely identify that individual (e.g., fingerprint, iris, gesture patterns). In order to deploy such systems, Universities generally need to license the technology from third parties. The cost and complexity is relatively high in comparison to non-technological alternatives, and a study by Levy, Ramim, Furnell, and Clarke (2011) concluded that student acceptance of third party vendor implementation of biometrics may prove problematic. In addition, recent disclosures about U.S. government monitoring of communications have created an increased media focus on privacy with regard to internet use (Luckerson, 2013). This increased public awareness and increase in demand for anonymity runs directly contrary to the concept of authentication and monitoring of remote users. Regardless of the need and appropriateness of deploying such technology, in the current public opinion climate, all actions toward individual identification and monitoring may prove difficult or impossible to implement.

Research staff from the ERAU Hunt Library assisted the author in performing an exhaustive literature search in this area; minimal quantitative data on student acceptance of authentication/monitoring technology was available. To address this lack of data, and to contribute to the general advancement of knowledge, an ERAU-W survey was developed to provide insights about the Worldwide-specific student body. Given the various approaches available for addressing the academic integrity issues, the apparent predilection of key accreditation and funding organizations for more robust solutions, and the specific conclusion of the Levy et al. (2011) survey, the author worked with the ERAU Office of Institutional Research to test the applicability of the Levy et al. (2011) conclusion to ERAU-W. The specific questions addressed through the survey were as follows: Will acceptance and adoption of biometric technology solutions be different among ERAU-W's unique student population from the resistance encountered in the Levy et al. (2011) study? To what extent do age, educational level, or military status affect respondent perceptions? Secondarily, the author attempted to elucidate other potential student body issues, such as usability of authentication technology and security/privacy concerns, which could have direct implications for the Ignite integration model as it relates to remote learning.

Methods

The author conducted an ERAU-W student body survey, sufficient in scope to address the fundamental question of third party biometric authentication, mirroring the aforementioned Levy et al. (2011) study. The survey questions and format were approved by the ERAU Office of Institutional Research in advance, and survey participation was entirely optional for all participants. The survey was sent via email to over 8,000 randomly selected ERAU-W students –

both graduate and undergraduate. Figure 1 is a graphical representation of the four research cells defined by the author.

	Questions relate to the use of biometrics and providing Embry-Riddle Aeronautical University with biometric data	Questions relate to the use of biometrics and providing Embry-Riddle's selected partners with biometric data
Video/Audio-related questions imply continuous monitoring of raw footage	RESEARCH CELL #1 Q1, 2, 3, 4, 5, 6, 7-1, 8-1, 9-1a, 10, 11	RESEARCH CELL #2 Q1, 2, 3, 4, 5, 6, 7-2, 8-1, 9-1b, 10, 11
Video/Audio-related questions imply monitoring of raw footage ONLY in the case of an anomaly being detected by a non-Video sensor, first	RESEARCH CELL #3 Q1, 2, 3, 4, 5, 6, 7-1, 8-2, 9-2a, 10, 11	RESEARCH CELL #4 Q1, 2, 3, 4, 5, 6, 7-2, 8-2. 9-2b, 10, 11

Figure 1. Key features of four independent (no repeat participants) research cells and corresponding question selections. See Appendix B for full questionnaire text.

All research cells were opened to accept responses simultaneously, from 4/23/13 until 6/9/13. The survey was originally planned to be conducted over one calendar month, but poor initial participation made it necessary to keep all cells open until such time as sufficient responses were collected to provide statistical significance comparable to the Levy et al. (2011) study, with comparable variance assumptions. Prior to undertaking the ERAU-W study, the author used the statistical variance results from the Levy et al. (2011) study as the basis for a Mathworks Matlab simulation of normally distributed participant responses, both with and without anticipated potential biases. Applying Analysis of Variance (ANOVA) techniques to these simulated responses using the OpenStat application, the author set a minimum threshold of 85 participants per cell in order to ensure that the resultant standard error of the means would be small enough to ensure meaningful insight into such biases within the general format of the survey questions – five discrete categories of response from "Strongly Disagree" to "Strongly Agree."

These discrete response choices were represented numerically, in the order and orientation originally presented in James, Pirim, Boswell, Reithel, and Barkhi (2006) – the journal paper cited for the formatting of the questions in the Levy et al. (2011) study. For some reason, this latter study chose to reverse the order and numeric values of the responses. The author did not suspect this of introducing a new bias, but reverting to the original response orientation allowed us to rule out any unintended effects due to the manner in which the responses were ordered.

Included as part of the invitation email sent to students was a link to a downloadable or web-viewable (via MediaFire.com) Microsoft PowerPoint Show (.ppsx) introduction to biometrics, lasting approximately ten minutes in duration. The purpose of the introductory presentation was to ensure a common understanding of technical fundamentals and terminology – how biometrics work, potential security risks, and privacy considerations. This introductory presentation is included in Appendix A. The link to the password-protected survey instrument was contained at the end of the presentation, thereby increasing the likelihood that survey participants would review the presentation material and subscribe to consistent definitions, prior to answering survey questions.

The survey instrument consisted of an online (administered through SurveyMonkey.com) questionnaire, comprised of 11 questions in length. The study attempted to differentiate between student acceptance of biometric authentication/monitoring for academic integrity as implemented by the University directly and the same technology implementation by a third party partner. Additionally, the study investigated differences in student acceptance of video/audio-based monitoring ("remote proctoring") versus non-visual sensors used to detect anomalies. The method of elucidating differences in student attitudes toward these variables involved presenting slightly different question wording to different, randomly-selected groups of participants. The precise wording of all questions used is listed in Appendix B. The study allowed the author to investigate correlations between age, military status, gender, and graduate/undergraduate status, respectively, and specific preferences expressed in the survey. The Internet Protocol (IP) address of each responding computer was captured by the survey instrument so that that computer would only be allowed to access the survey once (barring malicious attempts to corrupt survey results).

The total rate of participation in the study was 5.9% of all students invited. Of 476 student respondents, across the four research cells, 10 were removed from the study due to failure to fully complete the questionnaire. Because of the nature of the invitation email – linked to an introductory presentation which was in turn linked to one of the four cells in the survey instrument – the students were selected for a particular cell in advance of being contacted. A Mathworks Matlab script was developed by the author to generate uniformly distributed pseudorandom numbers. This script assigned students to cells by populating a linked field in an encrypted Microsoft Access database. As student contact information was added to the database, the student was assigned a random identifying key by Access and a research cell by Matlab. From that point on, only the student's email addresses were viewed directly. All other information about the student was masked by the identifying key. The participants in each cell were only provided links to view the questions associated with that specific cell. The introductory presentation content was the same for all cells, but four distinct presentations were used so as to provide four distinct links to the different cells of the survey instrument.

Both the introductory presentation and the online questionnaire were password-protected, so that only students invited to participate via email were expected to have access. Participant survey responses were maintained as confidential throughout. The questionnaire solicited student opinions with respect to the subject under investigation, but not personal information. The only participant-provided survey responses that could potentially constitute some form of identification were demographic in nature – age, military status, gender, grad/undergrad status. This information was only available to the author, maintained in the encrypted Microsoft Access database. Only totals and relative graphical representations are illustrated in this document.

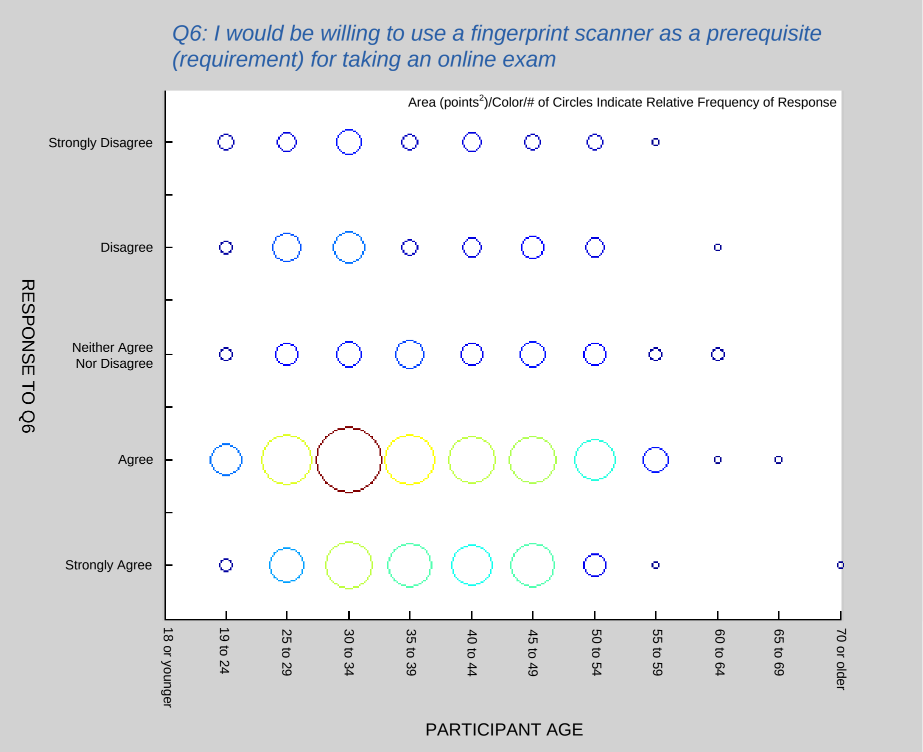


Figure 2. Correlation between attitude toward use of a fingerprint scanner and participant age.

Discussion

As the ERAU-W student body survey was designed to quantify opinions, generally on a discrete scale from 1 to 5, the summations of those opinions are presented graphically, on scatter plots and charts, which may reveal to the reader intuitive correlations between demographic data and the participant responses. Figure 2, for example, illustrates the greater frequency of “Agree” or “Strongly Agree” responses regarding survey question 6 – related to student attitudes towards fingerprint scanner technology – in the participants between ages 25 and 49.

The author also makes use of side-by-side comparison of results for similar questions, with slightly different terminology and connotations, in order to illustrate how participants may have responded differently to the choices of wording or how demographics may have played a role. By way of comparison, military status and gender (as illustrated in Figure 3) appeared to have no noticeable effects on the participants’ response to the use of fingerprint technology. Participants claiming some form of United States military service comprised 58.2% of the total respondents. Females comprised 18.2% of total respondents. In order to compare demographics when there was a disparity in the number of participants, the responses were first normalized so that the sum of all response frequencies for a given demographic were equal to all other demographics. Only the relative differences across demographics, then, are apparent in Figure 3. In addition to visual representations, the author provides a table summarizing key comparisons in sample mean and in inferential population standard deviation, after Figure 16.

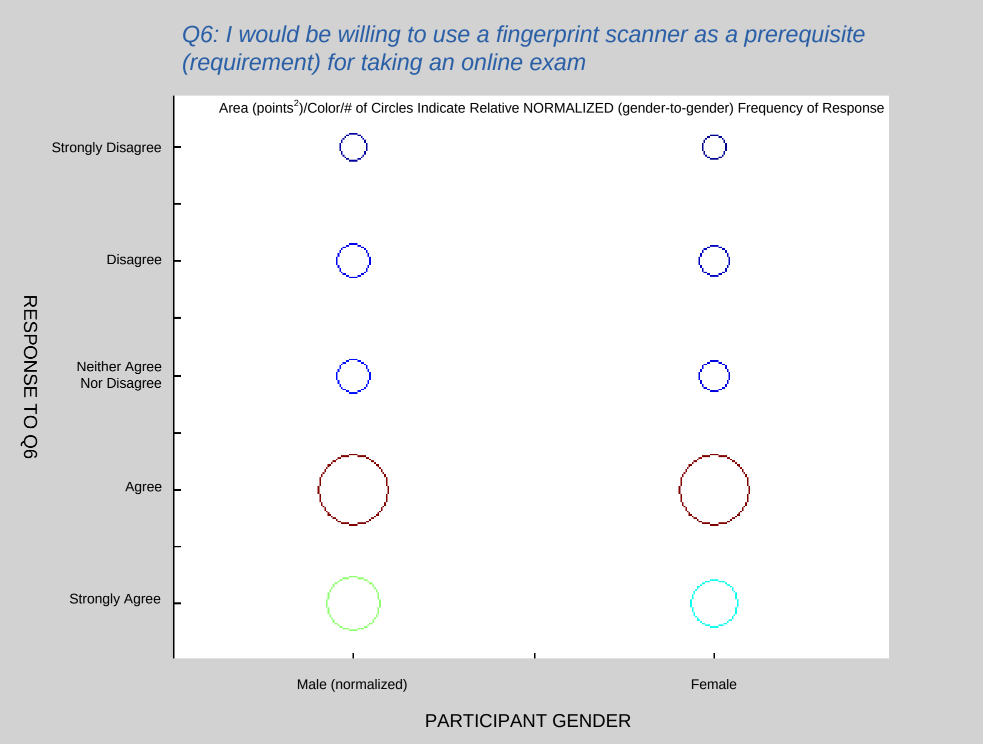


Figure 3. Male/Female normalized relative frequency of responses about fingerprint scanner are nearly identical although males represented a significant majority of the overall sample.

In the case of graduate versus undergraduate participation, graduate students comprised 56.4% of the total respondents. graduate normalized relative frequency of responses exhibited a small, but noticeable increase in positive attitudes toward fingerprint scanning technology vs. undergraduates. For undergraduate students, there appear to be less “Agree” and “Strongly Agree” answers and more neutral or negative answers, resulting in a shift of the sample mean, even though standard deviation for the two populations were relatively equal.

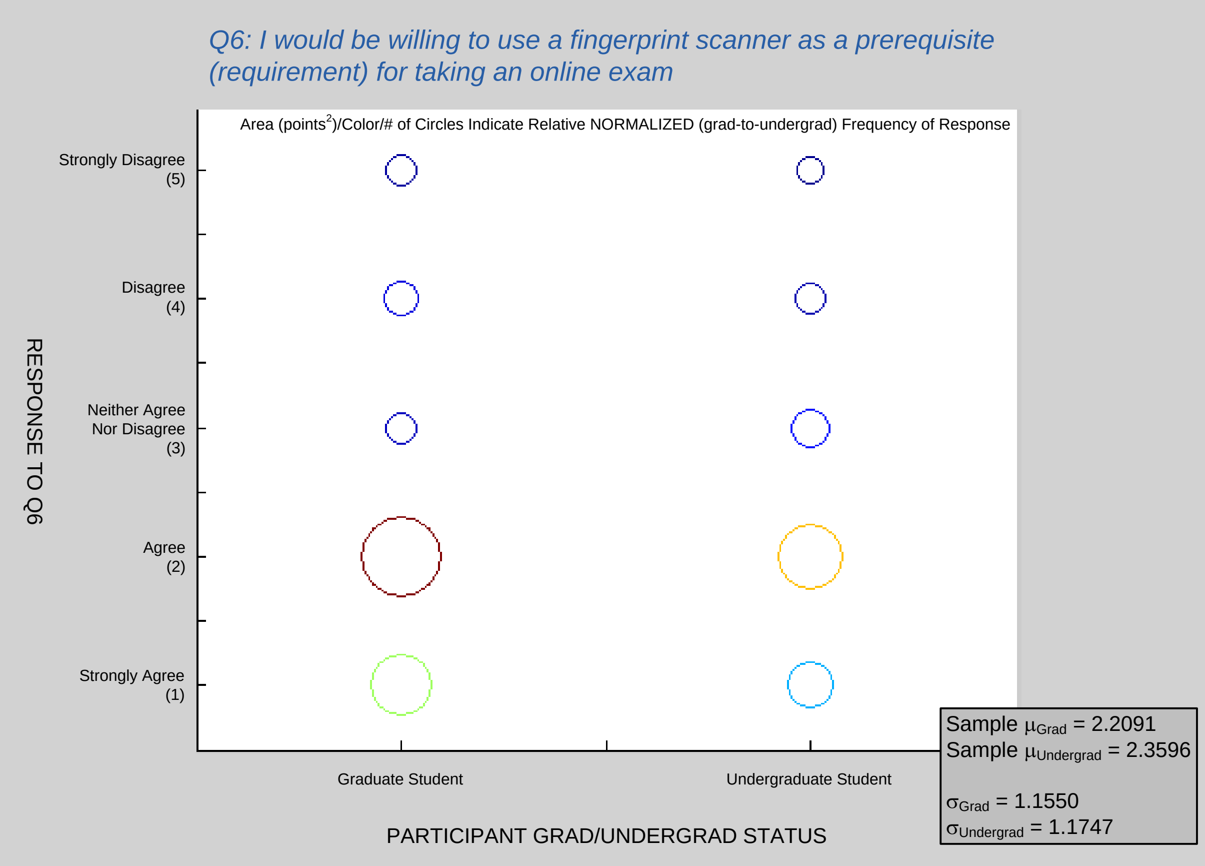


Figure 4. Relative normalized attitudes towards fingerprint scanner technology for exam academic integrity – graduate vs. undergraduate.

There appears to be only a slight difference between general agreeability toward fingerprint scanning – focused on the technology – and the institutional trust afforded to Embry-Riddle and ERAU's selected partners in implementing the fingerprint technology. Initially, the author was uncertain whether perception of usefulness or agreeableness towards a general technology would translate to trust in the institution using the technology or agreeableness towards the deployment. Figure 5 indicates that there is little noticeable disparity between user perception of the technology and user willingness to allow the institution to use the technology in the case of fingerprint biometrics.

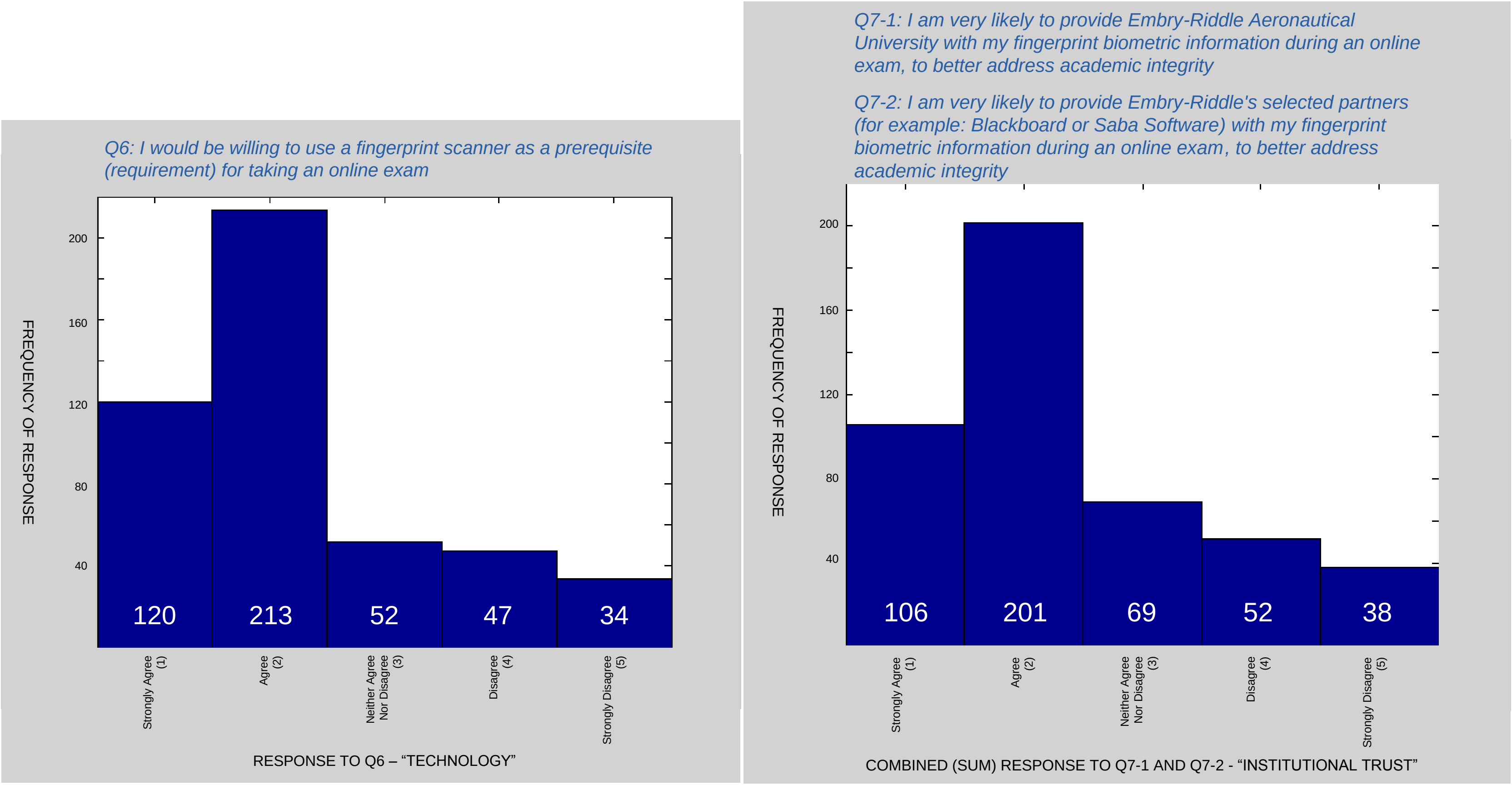


Figure 5. Histograms of student attitudes towards fingerprint technology versus institutional use of fingerprint technology – ERAU and selected partners.

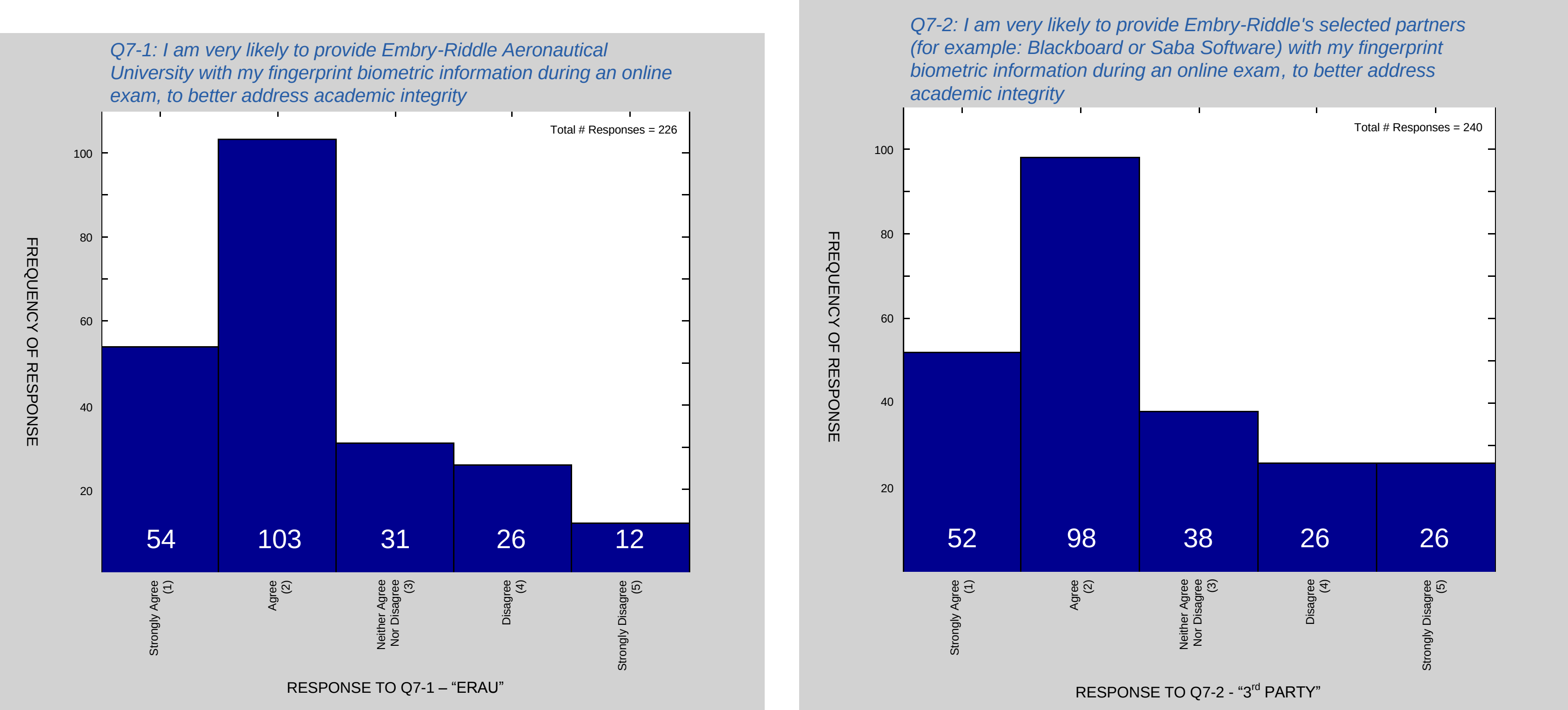


Figure 6. Histograms of student attitudes towards fingerprint technology implemented by ERAU versus ERAU's selected partners.

The two independent histograms look identical, with closely matching sample mean and standard deviation, listed in summary Table 1 (p. 30). The conclusion posited, then, is that the general ERAU-W student population would respond identically – agreeing or disagreeing with the use of the technology in general and with Embry-Riddle's use of the technology specifically – in approximately the same proportions as the sampled students. The link between third party implementation of biometrics and negative student attitudes, displayed in the Levy et al. (2011), is not apparent in Figure 6, in the case of fingerprint biometric technology. Though there is a slight shift in sample mean, it certainly does not appear to affect overall positive attitudes. This disparity with the Levy et al. (2011) study's results may stem from differences in ERAU-W's population or, perhaps, the phrasing of the ERAU-W study's question, which includes specific third party partners with which students already have some familiarity.

There appears to be a slight link between acceptance of video/audio and whether the video/audio is to be provided to Embry-Riddle or a third party. The histograms of Figure 7 mirror the conclusion of the Levy et al. (2011) study – that implementation of biometrics by third parties is sufficient to bias students' attitudes towards a negative response. The magnitude of the bias does not, however, appear to be as significant in the ERAU-W population as the previous study concluded. The use of video and audio, however, generates greater neutrality and even ambivalence in the respondent attitudes as compared to the results for fingerprint scanning.

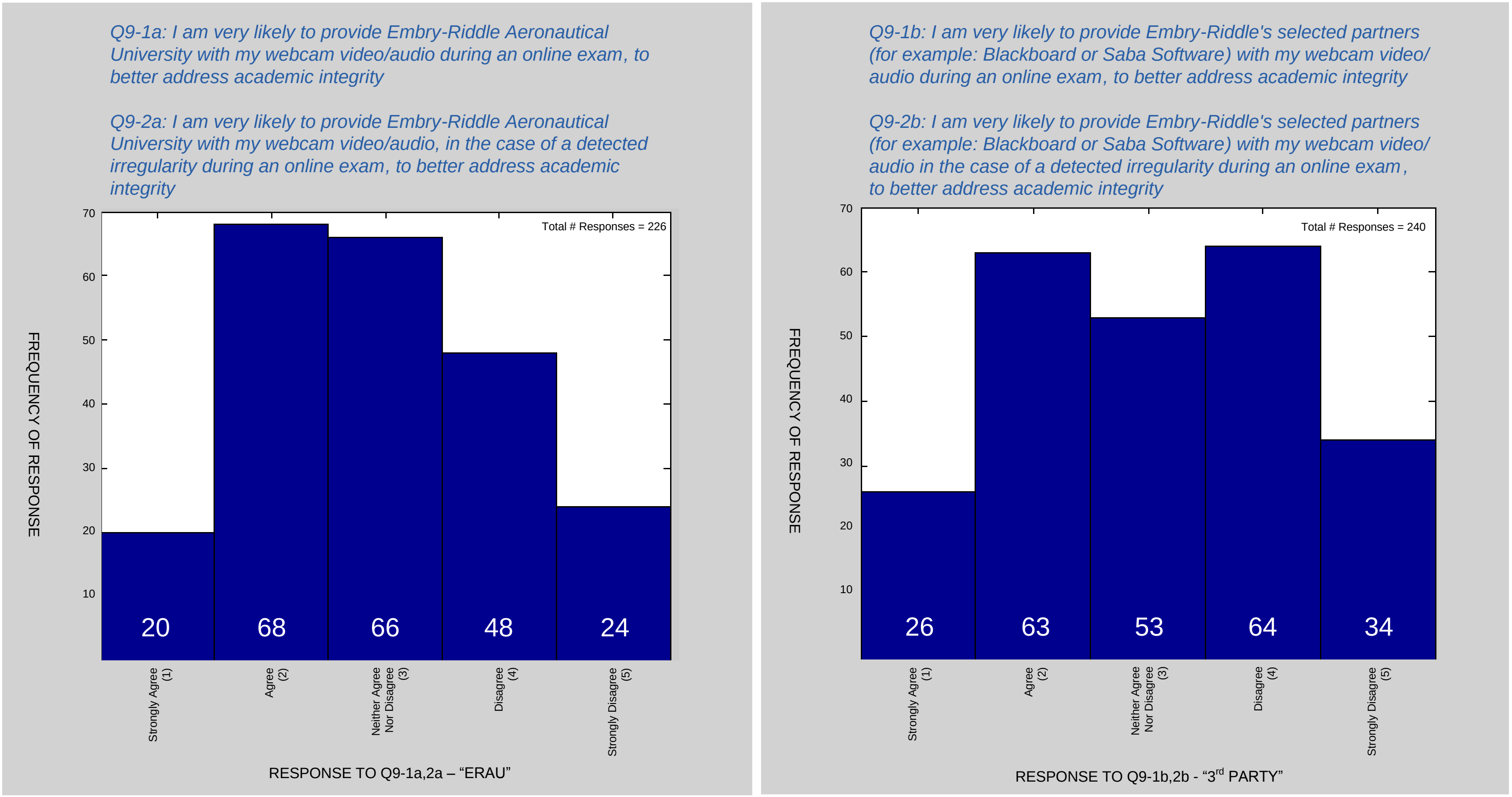


Figure 7. Histograms of student attitudes towards the use of video audio administered by ERAU versus ERAU's selected partners.

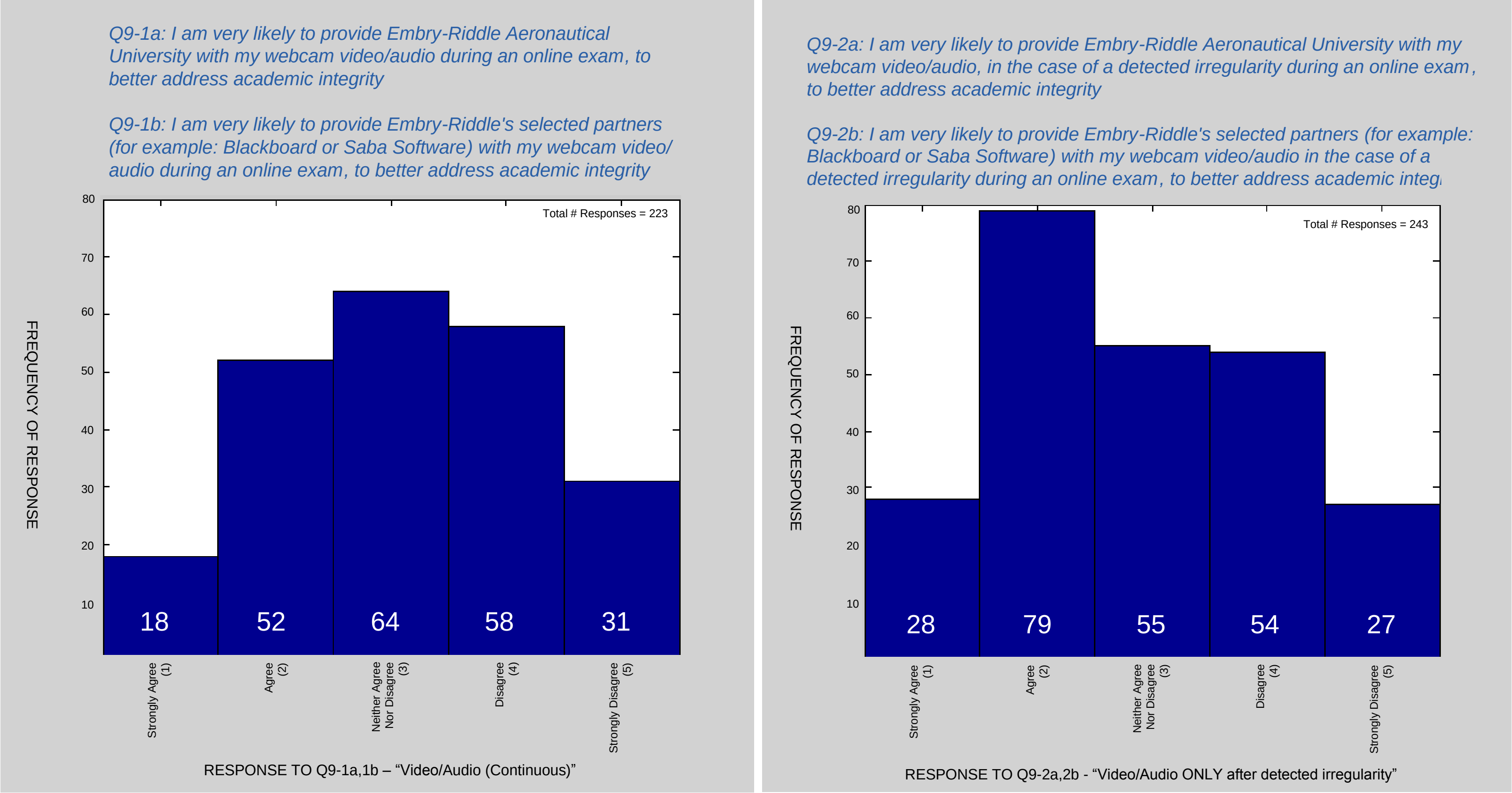


Figure 8. Histograms of student attitudes towards the use of video/audio in general versus the specific case of a detected irregularity.

Figure 8 appears to illustrate a link between student acceptance of video/audio biometrics and the knowledge that the video is only to be captured in the case of an irregularity being detected first, as opposed to unlimited use of video/audio.

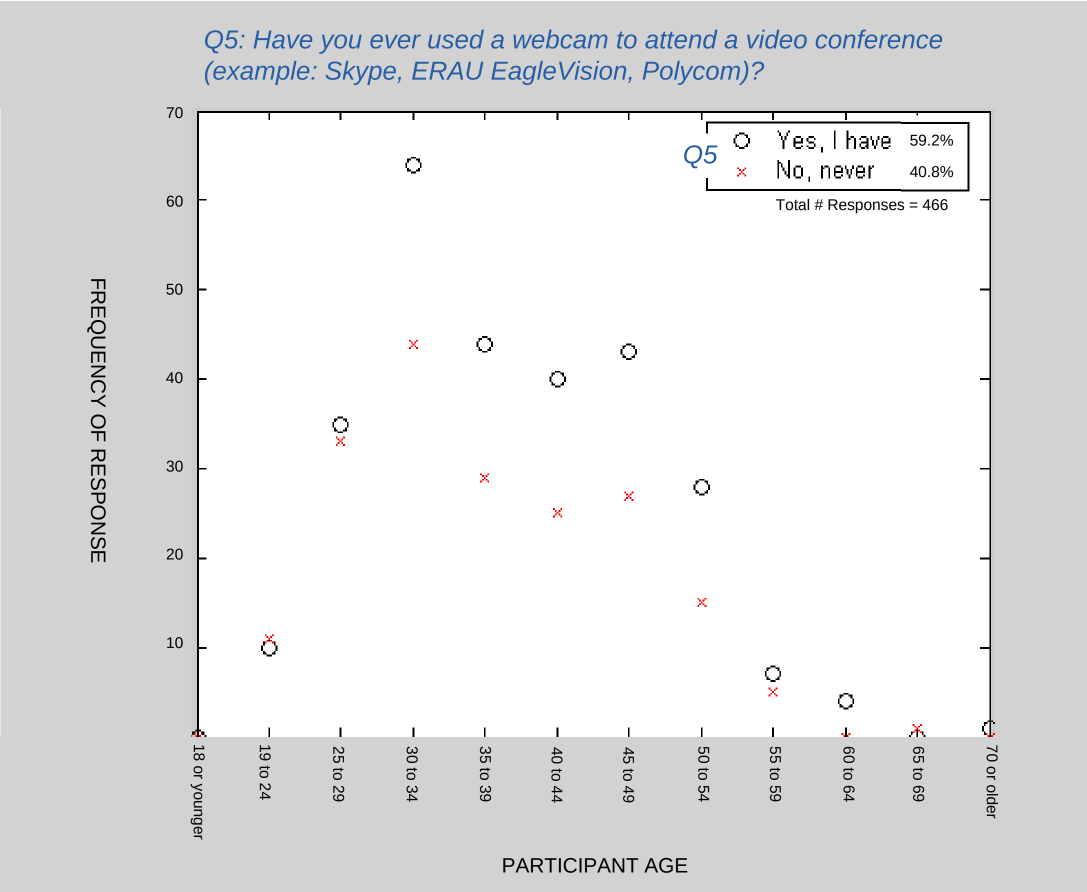


Figure 9. Scatter plot of student age versus frequency of participation – distinction between those with prior experience using video conferencing and those students who claimed no such experience.

In Figure 9, there seems to be a noticeable increase in the experience of using webcams among the age 30 to 54 participants. The author finds this increase to be intuitive, given the historical timeframe for deployment of video conferencing technologies and participants access to them. It is worthy of note, however, that even with the EagleVision modality offered by ERAU-W, only about 59% of students claim to have ever used this technology.

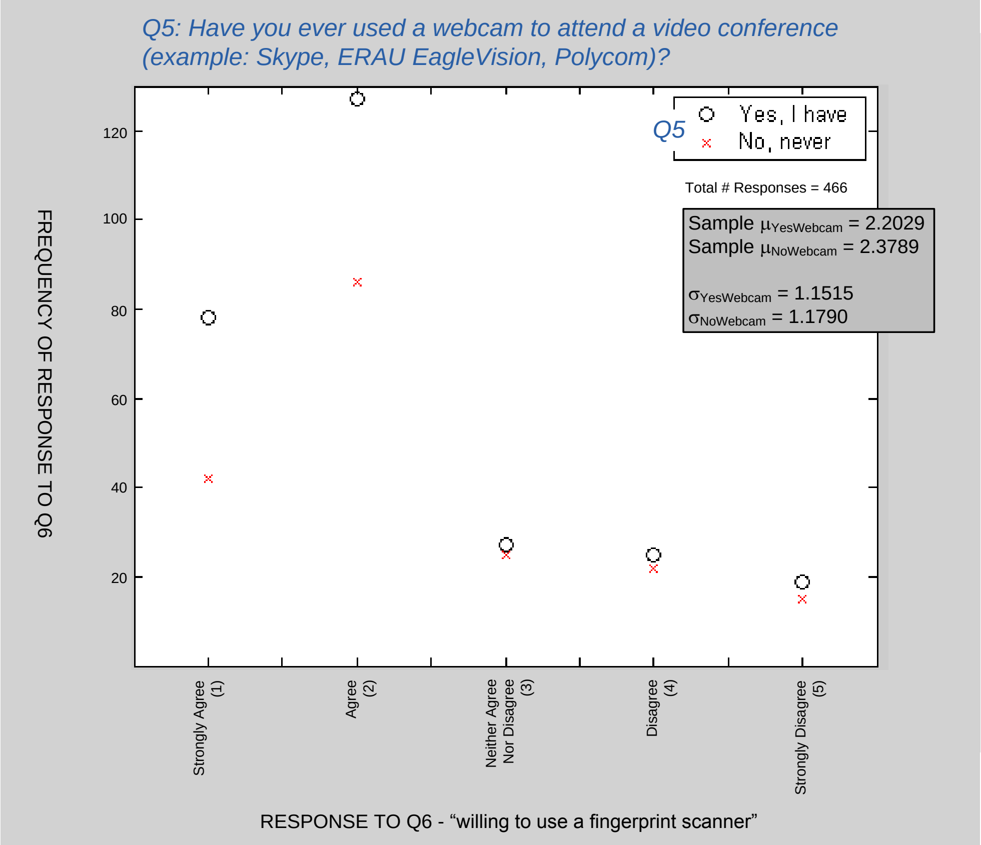


Figure 10. Scatterplot of student attitudes towards fingerprint scanners – distinction made relative to prior video conferencing experience.

From Figure 10, one can conclude that being neutral or ambivalent towards use of fingerprint scanners is a phenomenon independent of previous webcam/video conferencing experience. Agreeing or strongly agreeing, however, with the use of fingerprint scanner technology does appear to have some correlation with previous webcam experience. While correlations do not imply causal relationships, displaying the webcam information together with the same subjects' responses in relation to fingerprint scanner technology does lend interesting insight. The author interprets the implication of Figure 10 to be either that subjects with previous webcam/video conferencing experience would be more likely to elect to use fingerprint technology or that the nature of people willing to use fingerprint authentication technology is such that those same people would also be likely to make use of other network technologies, such as video conferencing. This has applicability to understanding the tendencies of EagleVision users.

Figure 11 shows an interesting trend. It has already been stated that approximately 59% of the student body has participated in a video conference via webcam – more participants having used the technology than not. The relative frequencies in Figure 11 are revealing. It would appear that attitudes towards the concept of a remote proctor being the equivalent of an in-person proctor – both positive and negative – appear to hover around neutrality or ambivalence, irrespective of prior experience with video conferencing technology. While those participants claiming webcam experience did shift the sample mean slightly towards neutrality, neither group demonstrated a positive attitude towards the technology. The author puts forward the theory, backed by student email comments, some of which were captured in Appendix C, that negative attitudes towards remote proctoring do not stem from technology concerns, but rather those of privacy/invasiveness/inconvenience.

With respect to the technologies addressed in this ERAU-W questionnaire, student responses implied a clear preference for fingerprint biometric over video/audio-based technology. Figure 12 shows comparative histograms of student responses relative to ERAU-W's deployment of each of these technologies. As it pertains to general pessimism towards third party deployment of authentication/monitoring biometric technology, the Levy et al. (2011) study does seem to capture student attitudes. The magnitude of the observed negativity, however, does not appear to be as pronounced with ERAU-W's student body. Figure 13 indicates the same student predilection for fingerprint scanning over video/audio monitoring, even in the case of third party providers. Video/audio clearly generated primarily neutral or ambivalent responses.

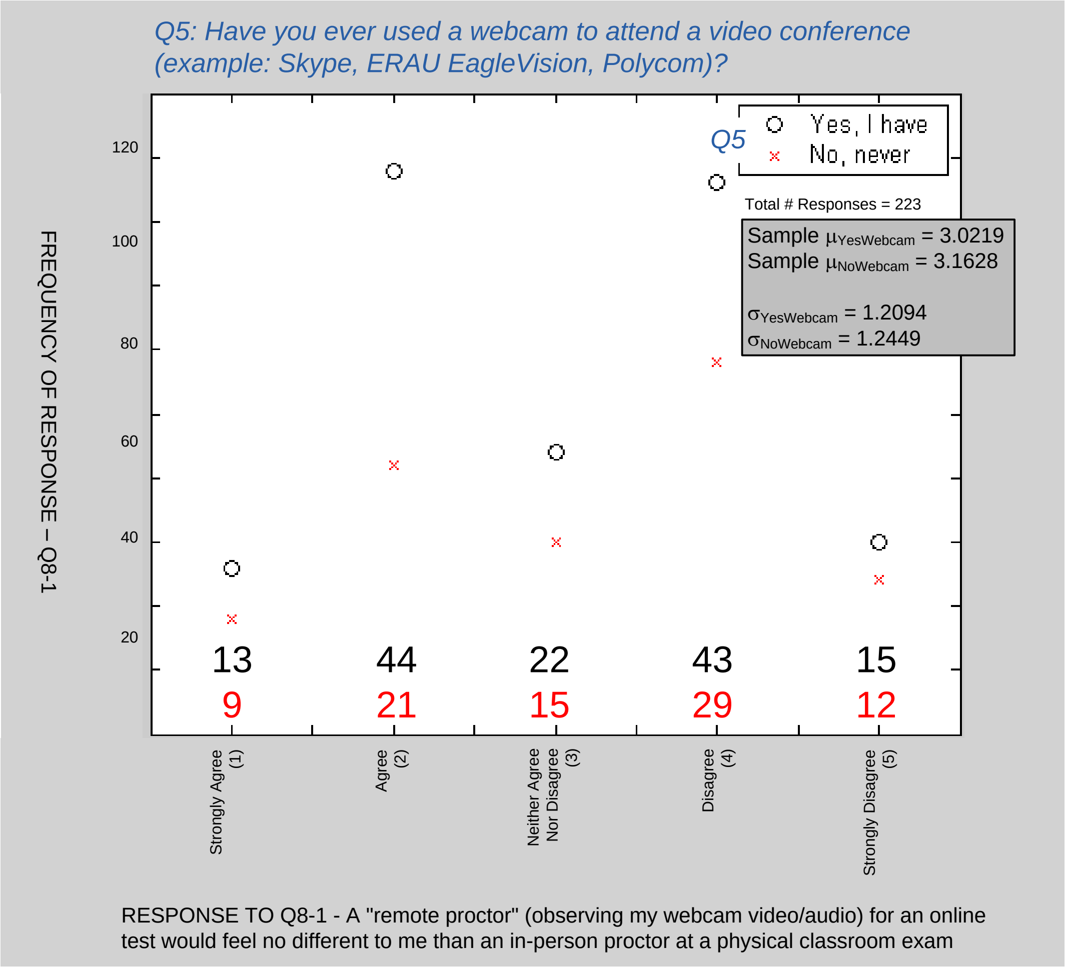


Figure 11. Scatterplot of students' agreement with equivalence of remote proctor concept versus in-person proctor – distinction made relative to prior video conferencing experience.

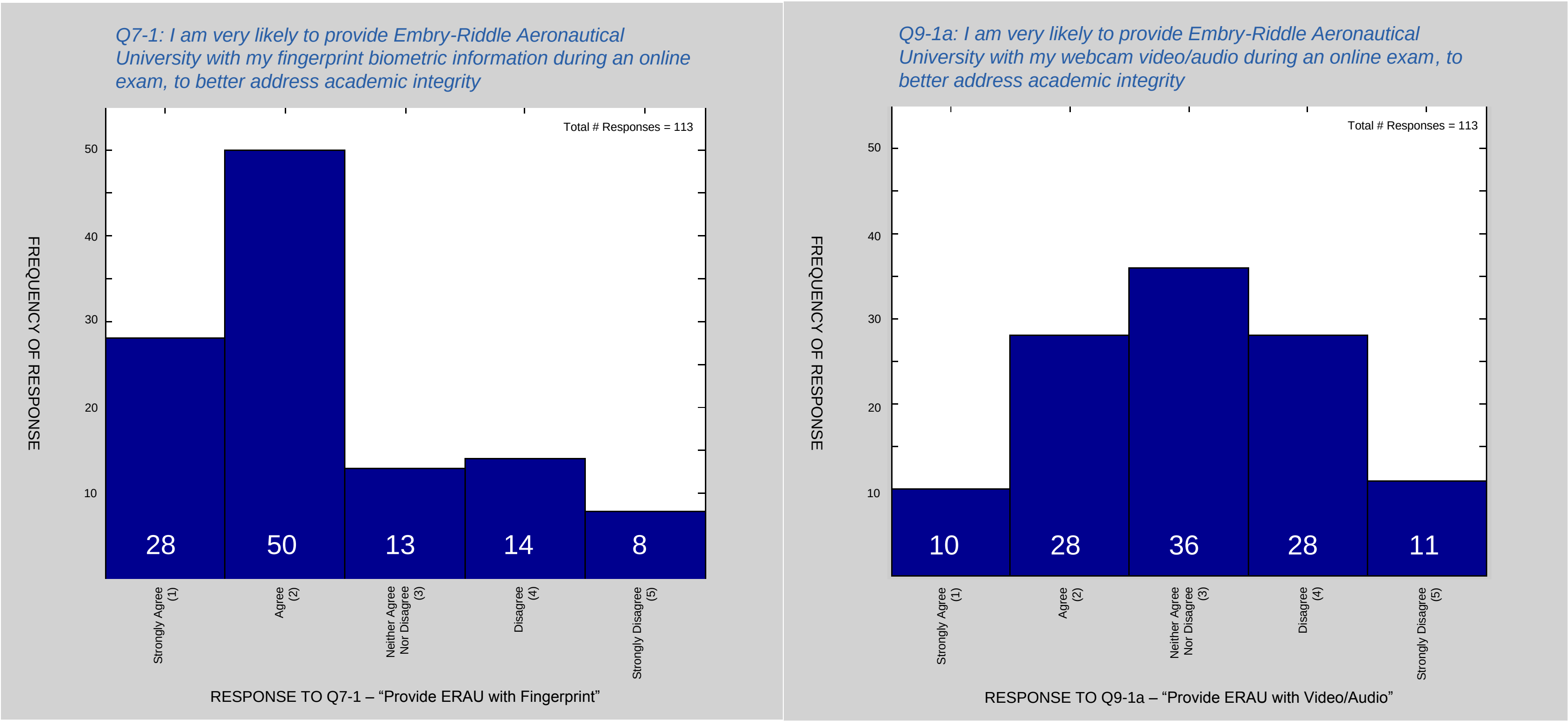


Figure 12. Histogram of student attitudes towards ERAU deployment of fingerprint scanning versus video/audio monitoring.

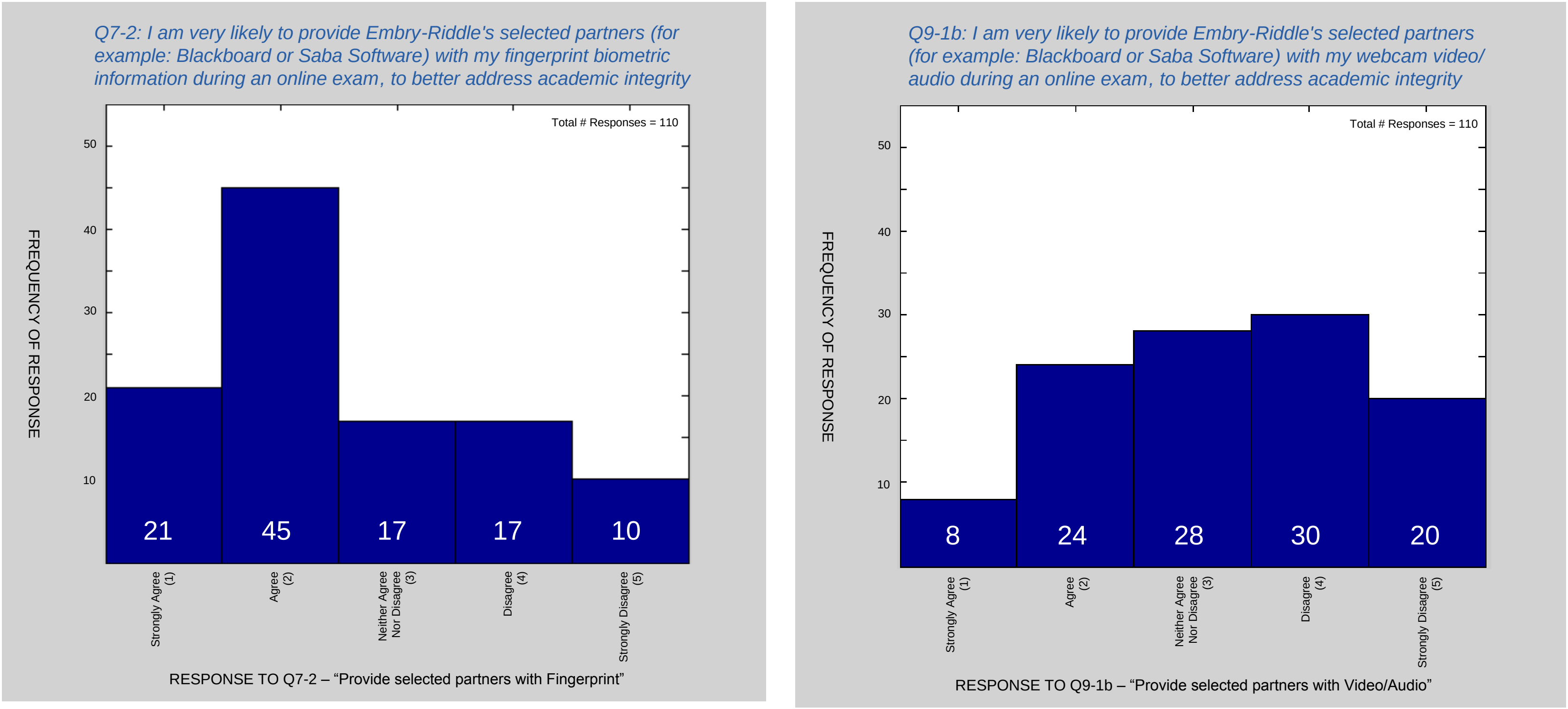


Figure 13. Histogram of student attitudes towards ERAU selected partner deployment of fingerprint scanning versus video/audio monitoring.

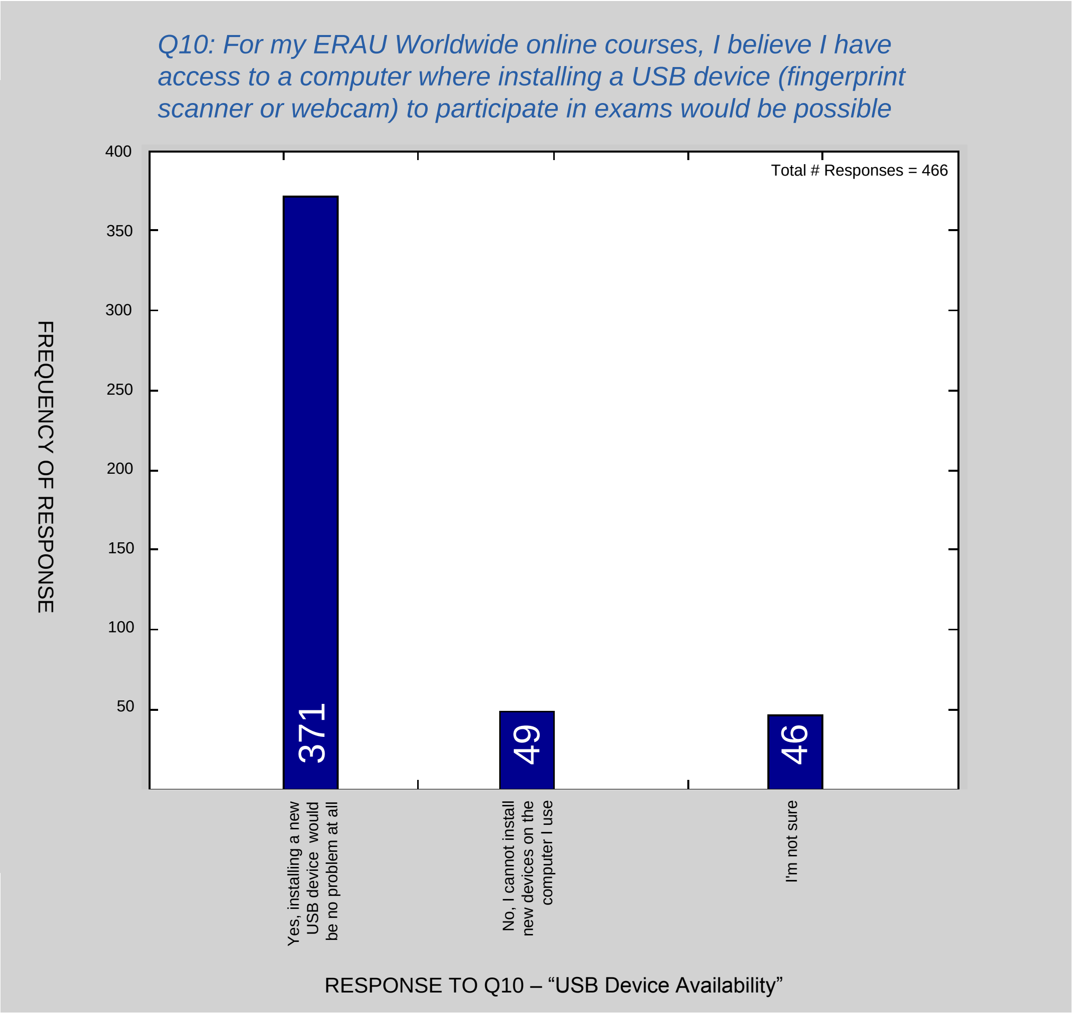


Figure 14. Chart of student responses with respect to the applicability of add-on USB devices.

In addition to technology preferences, cost, technical feasibility, and maintainability need be considered with any new deployment. In addition to increased network bandwidth usage associated with some USB devices, such as a webcam, a significant number of ERAU-W's students expressed either an inability or an uncertainty in adding any USB device to the computers they use for schoolwork. Figure 14 depicts this data, illustrating that nearly 20% of ERAU-W students could pose a technology installation problem.

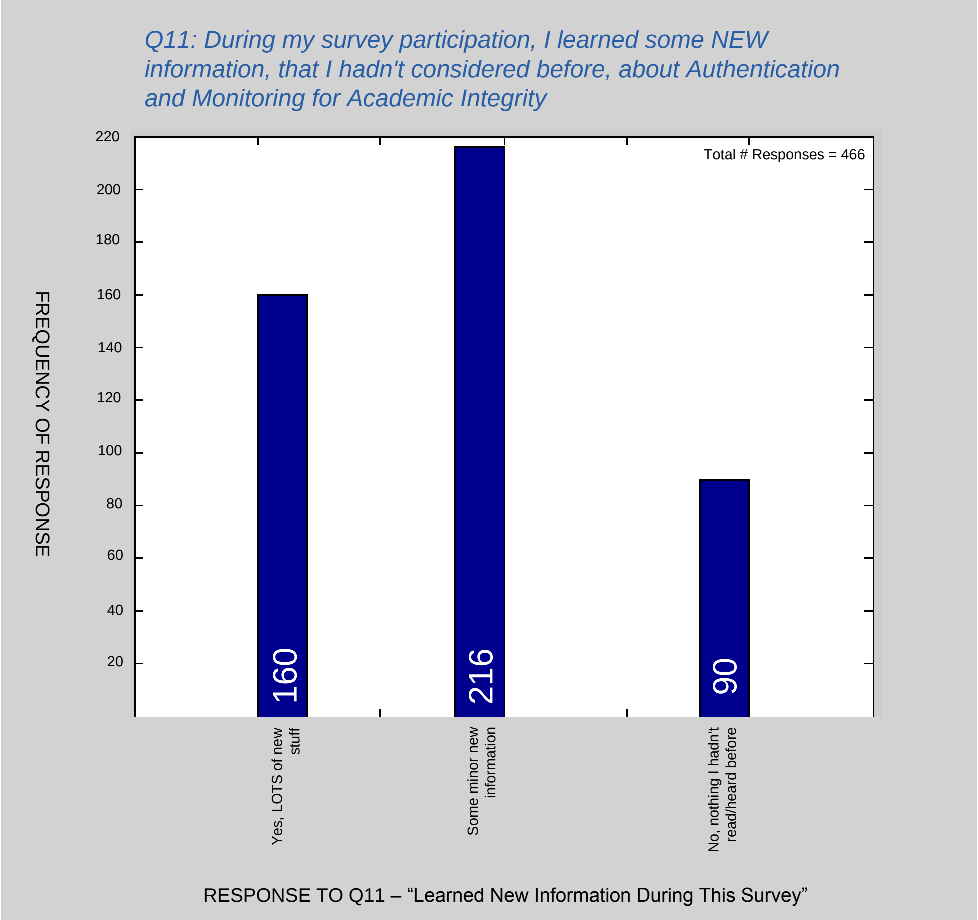


Figure 15. Chart of student responses about new information learned during the survey.

Figure 15 shows that over 80% of survey participants learned some new information during the course of the survey. This can be considered a positive for technology adoption, because it means that user opinions have not yet been fully established. There exists, potentially, a willingness to recognizing new information.

Figure 16 also illustrates what the author considers to be a positive outlook on the possibility of shaping student opinions. Reviewing the normalized responses for student knowledge gained (normalized number of respondents in each category: learned something significant new, learned minor new info, learned nothing new) versus the willingness to use fingerprint technology, it would appear that the most positive group was the group that believed they learned the most during the survey. The second most positive group was the group that believed they learned “some new information.” The least positive group could be construed to be the group that responded that they had not learned new information during their participation. Interestingly, this chart shows that in terms of relative frequency of positive and negative responses, the respondents who learned something new in the presentation – who felt they were introduced to the technology – were the most willing to use the technology. The author interprets this data as offering support for a general approach of offering education for students on the pros and cons and general considerations surrounding the implementation of new technologies. The concept would be intuitively similar to simply informing students that a campus library exists and that they must make use of the resource versus showing them the benefits of the library and providing coursework in which the use of library materials is beneficial. This is also an area where faculty mentorship can lend positive results. A student working with a faculty member that regularly uses biometric technology to access labs and research resources may find the technology less threatening than a student who has not been introduced to the technology by a trusted advisor or observed clear examples of the benefit.

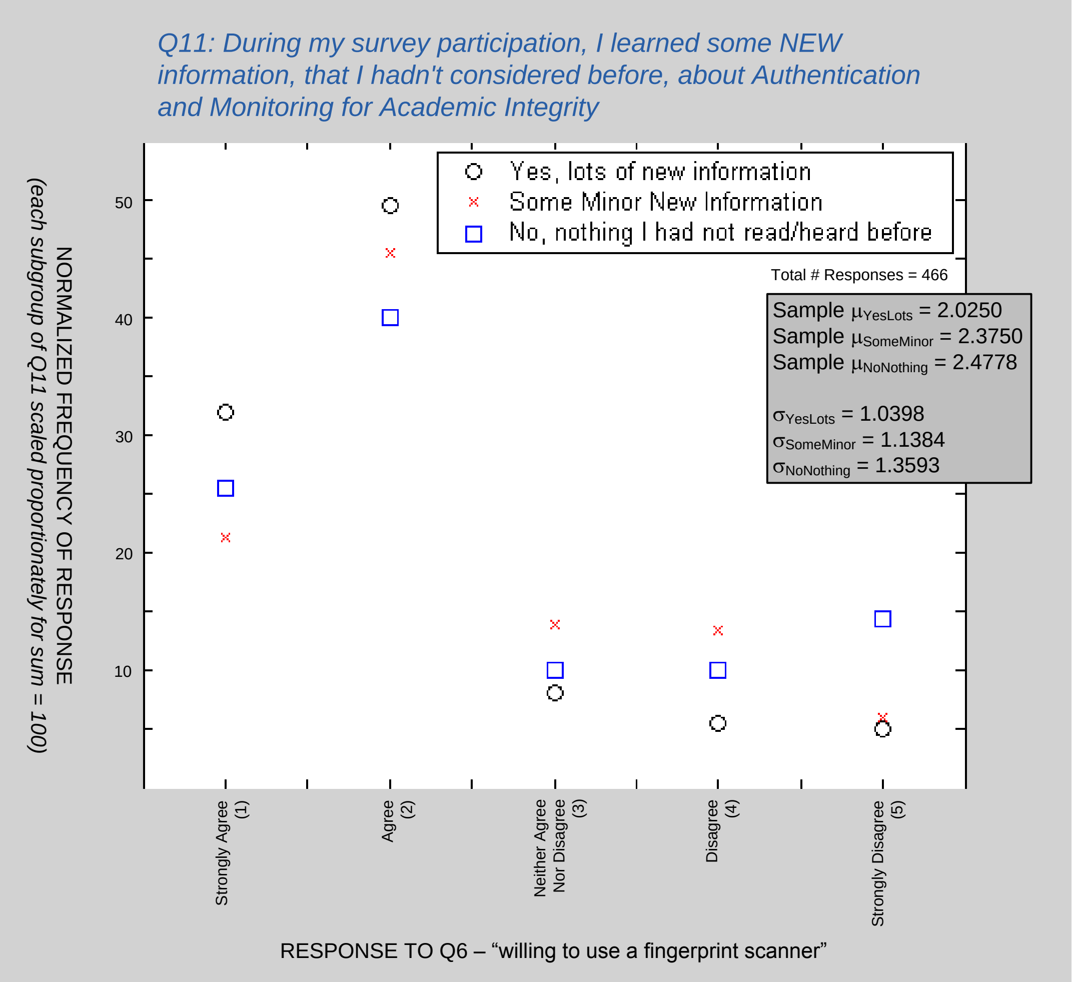


*Figure 16.*Scatterplot of students' willingness to use fingerprint scanning technology - distinction made relative to student learning of new information during the survey.

Table 1 offers a summary of key statistics and parameters related to student responses. Each row represents a comparison between similar or related pieces of information that the author chose to investigate. Differences in the sample means and standard deviations, across rows, tell us that students may have responded differently to the factors which the alternative wording of questions was meant to draw out. Similarly, when means and standard deviations are closely matched, this can be construed to mean that students did not respond differently to the differing factors in the questions.

Table 1

Summary of key statistics/parameters for responses reflecting student attitudes

Item under consideration (Data compared row-by-row)	Question	Specific factor emphasized in question	Sample mean	Std dev	Alternate question	Specific factor emphasized in alternate question	Sample mean	Std dev
Fingerprint biometric acceptance	Q6	General attitude towards Fingerprint Technology	2.27	1.16	Combined Q7-1, Q7-2	ERAU Institutional Trust with Fingerprint	2.39	1.19
Fingerprint biometric acceptance	Q7-1	ERAU-administered fingerprint	2.29	1.11	Q7-2	Selected-partner-administered fingerprint	2.48	1.25
Video/audio biometric acceptance	Q9-1a, Q9-2a	ERAU-administered video/audio	2.95	1.14	Q9-1b, Q9-2b	Selected-partner-administered video/audio	3.07	1.24
Video/audio biometric acceptance	Q9-1a, Q9-1b	Continuous video/audio monitor	3.14	1.17	Q9-2a, Q9-2b	Video/audio monitor only after detected irregularity	2.89	1.20
Technology Preference - via ERAU	Q7-1	ERAU-administered fingerprint	2.29	1.11	Q9-1a	ERAU-administered video/audio (continuous)	3.02	1.12
Technology Preference - via Partners	Q7-2	Selected-partner-administered fingerprint	2.48	1.25	Q9-1b	Selected-partner-administered video/audio (continuous)	3.27	1.20

Note. mean values ‘3’ = Neutral; ‘1’ = Strongly Agree; ‘5’ = Strongly Disagree

Areas for Future Research

The collected data meets the conditions for performing an ANOVA analysis of the data across the four cells of the study, using the OpenStat software package. ANOVA would provide a more quantitative representation of the statistical significance of the noted differences among cell responses. It would also allow for a direct comparison between Embry-Riddle's survey participants and the ANOVA examination previously applied to the sample population from the Levy et al. (2011) study. Similarly, although the survey well exceeded the sample size targets for each cell, we did not calculate effect size. Calculation of a quantitative measure, such as Cohen's d, will provide will lend insight as to the practical importance of some of the statistical differences thus far observed.

There are several variants of academic integrity technologies which were not addressed specifically in this high-level survey – among them voice recognition/identification and facial recognition. Making a distinction between video and audio, including the way they are used, could change student opinions of those technologies. In addition, some companies are specifically working on solidifying the security and integrity of test taking, going so far as to develop systems designed to operate and follow regulations involving student record data (FERPA) and commercial best practices with regards to the safeguard and transfer of personally identifiable information (Turning Technologies, n.d.). Investigating other available options, together with third parties, may be fruitful.

In addition, this survey was not fully encompassing in the area of biometrics; iris scanning, typing cadence/pattern recognition, and detection of anomalous behavior weren't specifically addressed. Knowing what level of invasiveness ERAU-W students would tolerate and accustom themselves to is important for future technology deployment.

From personal student insights that were shared via email (the vocal majority of which may not be representative of the entire student body, but nonetheless lend insight), concerns about biometrics seemed to be influenced greatly by concerns about security and data integrity, not so much the intended use of the technology itself. A follow-up study to refine this understanding and to provide a more robust explanation of potential security measures and University policies' effects in relation to negative student reactions is warranted.

It should be noted that some invited students – less than 1% – seemed to have a strong, even emotional reaction against their "privacy" being infringed upon, simply by being offered a chance to participate in this voluntary study. Certainly, if an email from faculty can be viewed as invasive to privacy, this is counter to the research culture the University is attempting to foster, and future studies or the deployment of biometric authentication/monitoring might be met with even harsher criticism from some students. The author is interested in whether something can be done in the future to allay those very strong reactions on the subject of privacy.

Conclusions

On a recent trip to an amusement park, the author's family was subjected to a fingerprint biometric scan. The scan was incorporated into the park experience, in order to make it appear enjoyable and innocuous, but the information captured and the ramifications were no less serious than a security background check or bank transaction. Airports have similarly promoted biometric scanning as a "privilege" rather than a requirement – offering the voluntary participant a faster route through security lines. Biometric usage will continue to expand in modern society.

ERAU-W has invested significant capital and intellectual resources to provide our students with the finest education and accredited degrees available online. The Ignite Integration Model will continue to steer ERAU toward a systematic, research-centric curriculum, which will only serve to spotlight authentication issues and the legal ramifications associated with policy that can quickly grow outdated relative to technology and the invitation of willful misrepresentation which remote learning appears to augment. Ironically, one of the fundamental research skills taught in any research methods course is that of evaluating sources – establishing the criteria used to determine the credibility and reliability of materials used in the research process. The same attention has not, as yet, been applied to validating human sources of information and intellectual capital in the educational realm. The Worldwide Campus has been ahead of the curve in distance education methods and technologies for years. The potential erosion of academic integrity represents a sophisticated technological threat that must be met with equally sophisticated study and response. No university serious about online instruction can afford to take this challenge lightly. Similarly, despite the difficulties and costs, no university can assume that the technology already being used at local amusement parks is too sophisticated for student body acceptance. Societal norms are changing.

Recommendations

The author makes the following seven recommendations for ERAU-W.

Recommendation 1. It has been explained (King, et al 2009) how clear statements of policy are viewed as a significant boon to academic integrity. Many respected universities continue to operate primarily on an honor system, but in the absence of clear, unequivocal direction, students' views of what is right/wrong become surprisingly (to this author and to those that conducted the King et al. (2009) study) flexible and, occasionally, self-serving. Policy statements – both of expected behaviors and of consequences for actions contrary to University expectation – influence the risk/reward ratio students perceive with respect to academic misrepresentation. The implementation of an ERAU-W student honor code, understood by all and signed by each student, is recommended.

Recommendation 2. The ERAU-W Instructional Design and Development team has made the author aware of course design approaches that fall under the heading of authentic assessment:

- Limiting the use of multiple choice questions
- Greater dependence on unique student projects rather than tests
- Capture of student and faculty work in easily accessible portfolio repositories, so that plagiarism is more readily detected.

All these approaches, the Online Exam Control Procedures (OECPs) listed in Cluskey et al. (2011), and the suggestions described in King et al. (2009) – not the least of which is the simple encouragement of active instructor involvement to reduce the likelihood of student misrepresentation – have been underway at ERAU-W and should continue to be explored and codified. Faculty mentorship is a core component in the implementation of ERAU's IGNITE integration model, because of the benefits to student motivation and the overall encouragement of research activities. Increased student/faculty face-to-face interaction also promotes academic honesty and integrity.

Recommendation 3. Ensure that policies consistent with and no less vigilant than brick-and-mortar universities for initial identification enrollment (drivers' license, social security#) are being followed, so that ERAU-W has a strong footing against the imposition of arbitrary/inefficient requirements from outside parties.

Recommendation 4. Begin actively engaging third parties on academic integrity technologies. Evaluate effectiveness, security and data-integrity, and cost of installation/maintenance as a necessary component of technology deployment. Perform voluntary pilot tests with EagleVision students and intentionally placed cheat subjects before deploying any new technology – leveraging the EagleVision students' inclination towards the early adopter mentality as the proverbial "canary in the coal mine". Example technologies to investigate

- Acxiom Identify-X – queries student periodically, based on information in public databases (drivers' license number, previous addresses, etc.)
- Respondus lockdown browser – limits access only to instructor-approved resources
- Remote Proctor Fingerprint Scanning Technology – deployed fingerprint biometric service with claims of secure networking/database to protect personal data
- Remote Proctor or ProctorU Remote Video/Audio Monitoring Service – exam recorded via proprietary webcam and USB driver/software (potential installation issue); reviewed by assigned specialists

Video/Audio monitoring appears to elicit the strongest negative responses from students and presents difficulty for military personnel and other students with unreliable network connections. These types of options should be evaluated, but considered for actual deployment only after other alternatives have been exhausted. In addition, the outsourced, third party proctoring service appears to be the least desirable option, given the initial ERAU-W survey results.

Recommendation 5. The author recommends caution in investigating technologies generally perceived as being more invasive than fingerprint (ex. iris scan, handprint); Student acceptance levels demonstrated in this survey and the current public opinion climate do not support adoption of such technologies.

Recommendation 6. With ERAU-W's strong record of working with military personnel, it would be worthwhile to begin jointly investigating USB port access as a limiting factor. Even simple deployment of the EagleVision modality requires a webcam. As less controversial, but necessary equipment becomes part of ERAU-W's day-to-day research and laboratory activities, investigating options for deploying USB connectivity for all students in a secure fashion will become increasingly important.

Recommendation 7. With any steps taken, communicate to the student body the nature of the deliberations and the consequences of both action and inaction. The participants exhibited strong, sometimes emotional responses to the survey topic. An author-selected, representative sampling of student comments - all received via email, separate from the actual survey instrument – has been included in Appendix C, so that the students' insights may be read in their own words. Both the quantitative data and the qualitative feedback give the impression that student attitudes can be swayed by clear communication and education.

References

ABET Engineering Accreditation Commission. (2012). *Criteria for accrediting engineering programs*. Retrieved from http://www.abet.org/uploadedFiles/Accreditation/Accreditation_Step_by_Step/Accreditation_Documents/Current/2013_-_2014/eac-criteria-2013-2014.pdf

Cluskey, G. R., Jr., Ehlen, C. R., & Raiborn, M. H. (2011).Thwarting online exam cheating without proctor supervision. *Journal of Academic and Business Ethics*, *4*, 1-7.

Embry-Riddle Aeronautical University. (2012). *Quality Enhancement Plan: 2012-2017.* Retrieved from http://spa.erau.edu/ignite/ignite.html

James, T., Pirim, P., Boswell, K., Reithel, B., Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the Technology Acceptance Model. *Journal of Organizational and End User Computing, 18*(3), 1-24.

King, C. G., Guyette, R. W., Jr., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *Journal of Educators Online*, *6*(1), 11.

Levy, Y., Ramim, M. M., Furnell, S. M., & Clarke, N. L. (2011).Comparing intentions to use university-provided vs vendor-provided multibiometric authentication in online exams. *Campus-Wide Information Systems*, *28*(2), 102-113.

Luckerson, V. (2013).The Anonymous Internet: Privacy Tools Grown in Popularity Following NSA Revelations. *Time Magazine*. Retrieved from http://business.time.com/2013/06/20/the-anonymous-internet-privacy-tools-grow-in-popularity-following-nsa-revelations/

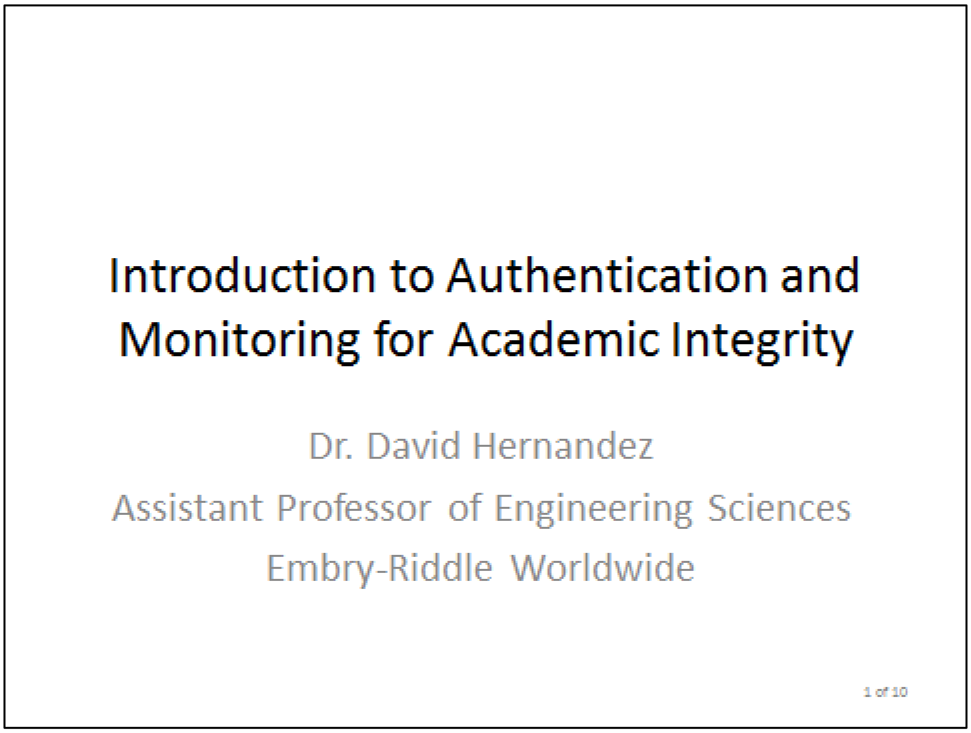
McConahay, M., & West, A. (2012).Establishing remote student identity: Results of an AACRAO/InCommon Federation survey. *College and University*, *87*(3), 59-66.

Semple, M., Hatala, J., Franks, P., & Rossi, M. A. (2011). Is your avatar ethical? On-line course tools that are methods for student identity and verification. *Journal of Educational Technology Systems, 39(*2), 181-191.

Turning Technologies. (n.d.). *Triton data collection system product details*. Retrieved from http://www.tritondatacollectionsystem.com/product-details

U.S. Department of Education. (2008). U.S. Department of Education Opportunity Act of 2008, HR4137(sec 496.B.ii), U.S. Department of Education, Washington, DC.

Appendix A
Introductory Presentation



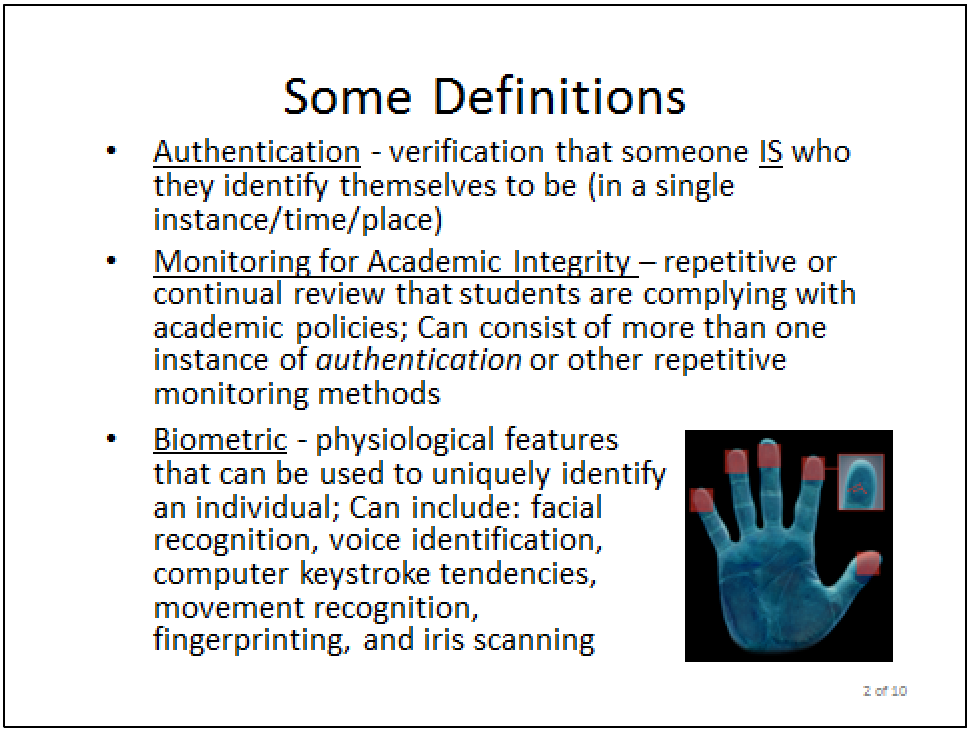
Introduction to Authentication and Monitoring for Academic Integrity

Dr. David Hernandez

Assistant Professor of Engineering Sciences

Embry-Riddle Worldwide

1 of 10



Some Definitions

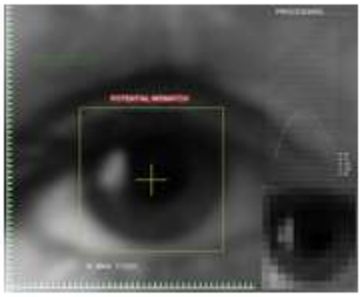
- Authentication - verification that someone IS who they identify themselves to be (in a single instance/time/place)
- Monitoring for Academic Integrity – repetitive or continual review that students are complying with academic policies; Can consist of more than one instance of *authentication* or other repetitive monitoring methods
- Biometric - physiological features that can be used to uniquely identify an individual; Can include: facial recognition, voice identification, computer keystroke tendencies, movement recognition, fingerprinting, and iris scanning

2 of 10

Becoming More Commonplace

- Non-University organizations and accreditation bodies, including the U.S. Department of Education, are taking an increasingly active interest in methods of Authentication, particularly for online, distance-education programs

- In order to grant access, Biometric Authentication systems compare the biometric provided during a "login" attempt versus the template created during user enrollment



Easily Integrated Into Everyday Life

- Biometrics can be collected via specialized sensors or even using everyday items like webcams, microphones, or computer keyboards

Pros/Cons of Biometrics

- Benefits of biometrics include:
  - **convenience** – this "passkey" is always with you (less to remember for the same or better level of security)
  - **security** – commonly expected that a properly implemented system will provide improved overall security as compared to non-biometric methods (passwords, keycards, etc.)
- Biometrics can also have negatives associated with them:
  - **individual discomfort** - perception of "invasiveness"
  - **privacy** - concerns over securing information from loss or misuse; Biometrics are biological features - not as easy to change as a typical password
  - **misuse** - how any biological information could be used in the future (to determine likelihood of a certain disease, for instance) is unknown; When you give your biometric, you are trusting the institution to use it ONLY for identification

Note: In a properly implemented system, it's impossible for any identifying information (including the biometric itself) to be transmitted outside the system

Monitoring for Academic Integrity

- Monitoring technologies during online exams can include a range of technologies - from asking the test taker repeated personalized identification questions (driver's license ID, mother's maiden name, date of birth, childhood home address, etc.) to sensing unauthorized use of alternate web pages (Google) during an exam

- Some companies even provide a "remote proctoring" service, where the assigned proctor observes a student's webcam video/audio during an exam

Eye of the Beholder

- Monitoring does not necessarily make use of video, but could rather comprise a combination of sensors and computing, based on knowledge of the user – known as "multi-biometrics"
  - Video games that accurately monitor body movement using sensors are becoming increasingly popular

  - Monitoring Example: detecting that a student's typing/writing style during an exam is inconsistent with their previous typing/writing style throughout the semester

Not new... Not going away

– The first commercially available biometric device (hand geometry) came to market back in 1976.

– Since then, there have been a variety of commercially-implemented applications for biometrics:

- Entry/security at some amusement parks
- Government biometric databases to get you through airport security faster
- Remote facial recognition for surveillance in casinos
- Fingerprint-based security to prevent laptops from being accessed by unauthorized users
- Medical applications using iris recognition to ensure medication/treatment is administered to correct patient

Online Survey

By clicking the link below, you acknowledge that:

- The purpose of the study, the procedures to be followed, and the expected duration of your participation have been explained to you.
- No payment will be provided, and possible benefits of the study have been described.
- You have had the opportunity to obtain additional information regarding the study and that any questions you have raised have been answered to your full satisfaction.
- You understand that you are free to withdraw consent at any time and to discontinue participation in the study without prejudice towards you.

- Take the survey here: http://www.surveymonkey.com/s/XXXXX

Password <ALL CAPS>: AUTH

THANKS, AGAIN, FOR YOUR PARTICIPATION!

- Dr. David Hernandez

References

- O'Leary, T. (2008). Acceptance and accuracy in biometrics. *Security Dealer & Integrator, Vol. 30*, Pg. 52.
- Wayman, J., Jain, A., & Maltoni, D. (2005). *Biometric systems: Technology, design and performance evaluation.* London, GBR.
- Adams, J. (2006). Biometrics: The keyboard has a good memory. *Bank Technology News,* Vol. 19(3), Pg. 31.

Appendix B
Full Questionnaire Content

Note: Each participant will be asked exactly 11 questions, in-total. The principal investigator will tailor the questions, as a function of the degree of participation and the ability to fulfill the mathematical requirements for analysis of specific cells.

Questions are numbered, with "-<#>" and "-<#><letter>" designations denoting possible alternative phrasing to be used in a different cell, with an independent group of randomly-selected participants.

1) What is your age?
   - 18 or younger
   - 19 to 24
   - 25 to 29
   - 30 to 34
   - 35 to 39
   - 40 to 44
   - 45 to 49
   - 50 to 54
   - 55 to 59
   - 60 to 64
   - 65 to 69
   - 70 or older

2) Have you ever served in any branch of the military, or not? <SM>
   - Yes, I have
   - No, I have not

3) Are you male or female?
   - Male
   - Female
4) Are you an ERAU-W graduate student?
   - Yes, I am currently enrolled in a graduate degree program
   - No, I am not currently enrolled in a graduate degree program

5) Have you ever used a webcam to attend a video conference (example: Skype, ERAU EagleVision, Polycom)?
   - Yes, I have
   - No, never

6) I would be willing to use a fingerprint scanner as a prerequisite (requirement) for taking an online exam
   - Strongly Agree
   - Agree
   - Neither Agree Nor Disagree
   - Disagree
   - Strongly Disagree

7-1) I am very likely to provide Embry-Riddle Aeronautical University with my fingerprint biometric information during an online exam, to better address academic integrity

- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

7-2) I am very likely to provide Embry-Riddle's selected partners (for example Blackboard or Saba Software) with my fingerprint biometric information during an online exam, to better address academic integrity

- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

8-1) A "remote proctor" (observing my webcam video audio) for an online test would feel no different to me than an in-person proctor at a physical classroom exam

- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

9-1a) I am very likely to provide Embry-Riddle Aeronautical University with my webcam video/audio during an online exam, to better address academic integrity

- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

9-1b) I am very likely to provide Embry-Riddle's selected partners (for example Blackboard or Saba Software) with my webcam video/audio during an online exam, to better address academic integrity

- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

8-2) A "remote proctor" (observing my webcam video audio ONLY in the case of a detected irregularity) for an online test would feel no different to me than an in-person proctor at a physical classroom exam

- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

9-2a) I am very likely to provide Embry-Riddle Aeronautical University with my webcam video/audio, in the case of a detected irregularity during an online exam, to better address academic integrity

- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

9-2b) I am very likely to provide Embry-Riddle's selected partners (for example Blackboard or Saba Software) with my webcam video/audio in the case of a detected irregularity during an online exam, to better address academic integrity

- Strongly Agree
- Agree
- Neither Agree Nor Disagree
- Disagree
- Strongly Disagree

10) For my ERAU Worldwide online courses, I believe I have access to a computer where installing a USB device (fingerprint scanner or webcam) to participate in exams would be possible

- Yes, installing a new USB device would be no problem at all
- No, I cannot install new devices on the computer I use

- I’m not sure

11) During my survey participation, I learned some NEW information, that I hadn’t considered before, about Authentication and Monitoring for Academic Integrity

- (1) Yes, LOTS of new stuff
- (2) Some minor new information
- (3) No, nothing I hadn’t read/heard before

Appendix C
Author-Selected, Representative Student Comments
(Received via Email, Separate from Survey Instrument)

"…my response was negative because at $495 per unit and an average of $200 per book per course I cannot afford to purchase any type of biometric ID device/video cam. Our household operates on cash debit only."

"Biometrics is going to be a good tool to increase authentication and fidelity of the online classroom."

"…3rd parties cannot be trusted with information in their possession. Blackboard cannot even upgrade their system without major inconveniences to worldwide students. Once an image/video is "out-there" there is no calling it back, privacy may be an issue with the video feed."

"In regards to the biometrics scanning type stuff, I'm not opposed to it in principle but I do have two concerns. First, I love ERAU but it is expensive. If this is something else I have to pay for then I would probably not like it…"

"I do business online so I trust large entities as far as using my financial data and such but I feel EARU would have to have a strong policy on protecting the bio data as well as some form of bond or insurance in case there is a leak. Also I think they would need an independent company to annually audit their procedures to be sure they are being adhered to."

"I would not participate in biometrics scanning if it was handled by a third part(sic) as I trust ERAU not someone else. I would in fact not continue my education with ERAU if they required biometrics and had it outsourced."

"You are NOT entitled to make any demands on me regarding surveys or anything else."

"…the military network will not allow for USB devices to be plugged in on the network. In some commands it will remove the computer completely from the network. For those in deployed locations that use the MILNET to access their classrooms, you may run into difficulty there."

"…I've also heard people bragging about their wives or others taking tests and doing papers. One student (not ERAU), boasted his wife did his entire master's degree for him -- start to finish."

"As for the video proctoring I have no issue with it I just don't see how that would work. ERAU has students in just about every time zone. One thing I love about ERAU is scheduel(sic) flexibility. If I had to adhere to a schedule so that someone could watch me test and such, I probably wouldn't be able to attend. When I did my undergrad with ERAU I had to drive 1.5 hours to their nearest extended campus to have exams proctored. I was fine with that because I still had the ability to schedule it when I was available."

“ an y of your students are military members or civilian DOD contractors or employees. On many occasions, these individuals are attempting to take your courses online while deployed. When deployed, these individuals are not able to access reliable, high speed broad band connections that would support heavy webcam network traffic…I myself have taken courses while deployed. Many times the videos and streaming medial(sic) are quite difficult using the satellite broadband connections.Please consider this factor as you look for solutions to academic fraud.”

“Over the last 8+ years, I've lived in Iraq and Afghanistan. As somebody who spent ~$80K on my twin bachelor's degrees, I was really offended at how pervasive and open the cheating is in online courses.”

“I would not have had any problem with biometric scanners prior to reading your power point presentation, but now I am unsure. No security is 100% and losing control of biometric information would be more serious than typical identity theft. If the US military cannot prevent their most secure secrets from being hacked, I doubt a college can guarantee the protection of any information they collect.”

“…my laptop has the capability to share video. I have the camera lense(sic) covered until such time that I need it, and here is why. When I work from home, sometimes I don't dress and shower for a couple of hours after I get up… I don't want my co-workers / classmates to see me in this state. Simple as it is, if it comes down to proctoring tests via video...I would probably rather go to the local campus and have one of them proctor… the convenience of this online course has allowed me… to enjoy and stretch my mind at my own pace.”

“I have enjoyed the online college experience. As a person working long and sometimes unpredictable hours the flexibility has been essential to my continued education (most of my schoolwork is done on the weekends), however I would have to give serious consideration to more conventional education if this is the future of online education, and I suspect it is. Unfortunately I cannot think of a better alternative to biometric scanning. If it were not for the security issue it would seem the perfect solution.”

“Something needs to be done. y degrees are being made worthless despite the huge investment in my time and my money. Essentially, the value of my degrees is being stolen -- there is no other way to describe this: theft.”

“Biometric authentication does offer the possibility of addressing some of this, but there are challenges. Down range the access rules change constantly, as do rules on the rights to install software or add USB devices. Internet access available one day, can then be blocked for weeks or months without notice.”

“…social networks, government agencies, and some workplaces have too much information and feel a certain entitlement to that. I would hate that my school would also get to that point.”

“This is scary for me because in order for any of these devices to work they must turn whatever information they gather (retna[sic]scan,finger print, voice recognition) into a digital file or packet; what safeguards would be there to make sure it wasn’t accessed by unauthorized users? …The only reason why I would agree is that I feel like it gives my online education that much more credibility. So far in my studies at [E]mbry-[R]iddle I have never doubted the value of my courses, but there are those in our world that look down on an online education and feel like it is somehow not earned with the same level of accountability as an in person type of program. I would do anything I could to improve the image, and therefore add to the value of the degrees that all of us are earning.”

“…I like that it is an area of research and think that as distance learning continues to evolve from its primitive form of videoconferencing on a one-to-many model to the modern distributed classrooms, anti-cheating solutions should evolve as well.”