Association of Test Publishers' Security Committee (ATPSC)
PRIVACY IN PRACTICE BULLETIN
A Publication of the ATPSC International Privacy Subcommittee

To read all published bulletins visit: https://www.testpublishers.org/atp-security-committee-reports

For more information contact:

Bulletin 9
April 7, 2020

PRIVACY CONSIDERATIONS IN ONLINE/REMOTE PROCTORING

Moving High-Stakes Testing Programs Online Calls for Privacy Measures

NEED FOR ONLINE/REMOTE PROCTORING

Due to the rapid emergence of the COVID-19 pandemic, with so many people working and/or studying from home, testing organizations are evaluating the option to use remote technologies to replace "in-person" testing. These constraints are increasingly coming into play for many test sponsors/ programs ("test sponsors") that deliver high stakes assessments, whether as part of critical certification or credentialing programs or in higher education. Instead of monitoring testing events in a test center, where proctors are present either in the room itself or are watching from an adjoining area, organizations are turning to Internet-based online/remote proctoring. Proctors may be humans provided by the test sponsor itself, provided by a third-party service vendor, or may be non-humans conducting automated monitoring of test takers. Even some remote proctoring services are changing their method of operation because proctors themselves must work from home (i.e., a "remote/remote proctor" using sharing technologies such as WebEx, GoToMeeting, or Zoom). A proctor may watch the test taker in real time through a video connection ("live online proctoring"), record the test taker during the test administration and review the video later ("record and review proctoring"), or use a combination of both methods. Indeed, these methodologies were being used prior to the COVID-19 pandemic, but their use is quickly expanding to include many high-stakes tests. Just like an in-person proctor, a remote proctor (whether human or automated), supervises the integrity of the testing process and flags anomalies that could indicate test cheating.

Medical experts advise that at least some of these testing constraints are likely to continue for the next 18 months or more—until a COVID-19 vaccine is developed, tested, and administered widely. It is possible that localities will be able to ease some of the restrictions (e.g., lockdowns, school closures) intermittently during the coming months, but other restraints (e.g., social distancing, limits on large gatherings) may well continue into 2021. Under these conditions, a significant number of test sponsors will not be able to administer their tests in the usual manner. Even if some of the most rigorous restrictions are lifted, prohibitions on large gatherings are likely to remain. Attempting to administer a test to a large number of test takers in a single room, or to hundreds of test takers in a test center, could endanger the test takers, staff administering the exam, and the public health in general. Setting of a test date across multiple jurisdictions will also be made difficult because of the differences in the timing of virus outbreaks and public health responses. Thus, using online/remote proctoring has become the preferred option for many testing programs.

PRIVACY CONSIDERATIONS

Because of unique circumstances surrounding online/remote proctoring, it is necessary for a test sponsor or other testing organization (as the "controller" that makes decisions about what personal information to collect and how to use it) to address a number of related privacy considerations.[1] Depending on the jurisdiction(s) in which your program operates, there may be additional requirements imposed by law. This Bulletin is largely based on privacy considerations found in the General Data Protection Regulation (EU), the Personal Information Protection and Electronic Documents Act (Canada), the Family Educational Rights and Privacy Act (US federal law), and the California Consumer Privacy Act (US state law). As such, while there may be some differences between jurisdictions, if your testing program is international in scope, you should try to reconcile your privacy decisions as much as possible with the following eight considerations.

A. Purpose for Collecting Personal Information

As a general rule, almost all privacy laws/regulations require that the test sponsor/controller provide a test taker with an explanation of the types of personal information collected and the purpose(s) for which it is used. Thus, in order to ensure that online/remote proctoring is being conducted in accordance with applicable laws and/or regulation, the controller, as well as its processor(s), and any sub-processor(s), need to document all personal data collected and processed during the proctoring process.

It is equally important to remember that the concept of data minimization should be applied to the greatest extent possible; that is, personal information that is not absolutely required for online/remote proctoring should not be collected. Therefore, you should evaluate what personal information is truly needed for the functioning, integrity, or security of your assessment process. As discussed in Bulletin 8, "Privacy By Design and By Default – Demystified" (January 2020), controllers and processors also should follow the principles of privacy by design and privacy by default so that only personal information which are necessary for a specific purpose related to proctoring are processed.

Equally critical, there are rules about personal information that is considered "special" or "sensitive" under the laws or regulations of jurisdictions in which the tests are delivered – and this often includes biometric data if used to uniquely identify test takers. Accordingly, if your online/remote proctoring includes the collection and processing of biometric data to identify individuals or indicates behavioral patterns of the test taker, you will likely be required to treat such data

[1] For the sake of brevity, terms previously defined in earlier Bulletins will not be repeated here.

with special protections.[2] Finally, personal information that is processed during proctoring may not be used for non-assessment purposes without such use being disclosed to test takers.

B. Communications with Test Takers

As stated above, the test sponsor/controller need to communicate with the test taker to provide all of the required information about its decisions regarding the collection and use of the test taker's personal information.

In advance of taking the test, the controller must provide the test taker with clear and easy to understand notice of the types of personal data being collected as part of the proctoring process, how it will be used, how long it will be retained, the geographical area(s) in which it is processed and/or stored, how it will be safeguarded, and to whom it is disclosed/shared (*see* Section D) and why. Often times, this communication is made through the organization's Privacy Policy. The controller also needs to give clear instructions on how to contact the controller to raise questions, issues, or concerns.

The controller must have a privacy policy that the test taker can review and a process for the test taker to know what personal information has been collected, as well as a process for how the test taker can request a copy of his/her personal information and/or correction or deletion of his/her personal information. Finally, the controller needs to explain when the test taker's requests may be denied (e.g., if information needs to be retained for legitimate test security reasons).

C. Data Retention and Deletion

A controller needs to establish a retention policy for how long the test taker's personal information may be retained. The retention period for some types of data (e.g., copies of government identity documents) may vary from that used for less sensitive data. Similarly, the length of retention of sensitive personal information (e.g., biometrics) may need to be considered separately (see Section G, discussing Video Surveillance). Detailed proctoring information on test takers where no irregularities are involved should be retained for only a short period.

After the retention period, the controller (directly or via a processor) should destroy personal information promptly. Technical measures (see Section F) should be used to ensure that the deletion is irrevocable. Any delay in destroying the data should be reported to affected individuals within 30 days of discovery. If a controller terminates a contract with a processor, the controller should direct the processor/service provider to return or delete all the personal information it holds.

[2] The EDPB Guidelines (*see, infra.,* Section G) on the use of video surveillance advise that video data is not necessarily special categories of data so long as that it is not used to determine special categories of data or to identify people.

D. Sharing Personal Information

A major issue under various privacy laws and regulations is how the personal information of test takers is shared by the controller between it and its service providers/vendors and ultimately to third parties (e.g., employers, certification bodies). Generally, the controller needs to ensure that all its service providers/processors are operating under a contract that ensures that any test taker personal information that is collected or shared is ONLY used for the purposes of fulfilling the contract with the controller. In other words, if an online/remote proctoring service provider collects or receives personal information of a test taker, it must be sure not to use it outside of the contract with the controller for its own purposes, especially for any marketing or promotional purposes. In other circumstances, when the test taker contracts for testing services, it should be made clear that "processing of your personal information is necessary for the performance of this contract."

The controller also needs to document the geographical locations in which it stores personal data, including through the use of cloud services, and ensure that any personal information that is exchanged across territorial boundaries is done in a way that complies with applicable privacy laws/ regulations.

E. Automatic Decision-making and Artificial Intelligence (AI)

Where the proctoring services use or are dependent upon automated decision making (e.g., machine learning, algorithms, AI), that fact must be communicated to the test taker, along with information about how the automated decision-making is used (e.g., reasonable explanation of how the automated decision-making occurs).

Where any decision is made as a result of using automated means (e.g., a decision to flag a test taker for possible cheating or a decision to stop the test due to possible cheating), the controller (directly or via the processor) should ensure that the algorithm used is subject to thorough and ongoing evaluation for fairness and quality.

The controller, or any processor involved in the use of automatic decision-making, should take appropriate steps to minimize the risk of errors and to prevent bias and discrimination. Enabling the test taker to appeal to a human reviewer as to whether an automatically made decision was fair and appropriate needs be in place.

F. Technical and Organizational Measures

Controllers and processors need to take appropriate technological and organizational measures to protect test takers' personal information from destruction, loss, and alteration as well as from unauthorized disclosure, access, or processing.

As discussed in Bulletin #7, "Security Standards and the Assessment Industry" (January 2020), such measures should be aligned with ISO 27001 and ISO 27701, and/or with SOC 2. Some controllers and processors may wish to obtain a third-party certification against those standards, as well as to regularly evaluate their information security measures.

These measures are likely to include a decision by the controller and/or processor to encrypt all test taker personal information in its possession both at rest or when transmitted, using strong encryption techniques (or otherwise securely protecting data in transit to avoid interception).

Access within a testing organization to personal information should be limited to those with a need to know, which is usually limited to a very small number of people. Ensuring physical security in an organization's own facility also may be a consideration.

Finally, it also may be practical to store personal information collected during the registration and used in the proctoring process to be held in a pseudonymous format (e.g., associated with an ID), rather than directly with assessment participant name. While pseudonymous data in some instances is still considered personal information, it does provide additional security in protecting against easy access to it.

G. Use of Video Surveillance

All forms of online/remote proctoring use video surveillance (e.g., standard computer webcams or additional video mechanisms). Remote proctoring with use of video helps ensure that the right person is taking the test without help and that the test is taken without unfair aids. In some cases, video is used to allow the proctor to monitor the test taker in real time with or without recording; in other cases, recording is used to permit review at a later time. The other considerations in this document apply to video personal information in the same way as to other kinds of personal information.

Most testing organizations (the controller and its proctoring service provider) will generally articulate a "legitimate interest" to justify use of video in this context (i.e., the reason for video surveillance is to protect the rights of ALL test takers in obtaining a fair and accurate score, as well as to discourage and reduce cheating, and to protect their interest in the test materials). In an online/remote proctoring environment, the controller should document its interests and explain why these are not overridden by any privacy interests of the test takers being taped – it is not sufficient just to say the organization's interests are legitimate without documenting a proper justification. This should be in the form of a written legitimate interest assessment ("LIA") which addresses the purpose of recording and reviewing video, together with the necessity to use video as opposed to

alternative ways of achieving the same purpose and any measures that may be taken to limit the extent and intrusiveness of the processing.[3]
The LIA requires a testing organization to balance the interests of the test taker who would be under surveillance against the organization's identified legitimate interests, considering factors like the nature of the personal information involved, the reasonable privacy expectations of the test taker, and the likely impact of the video surveillance on an individual test taker.[4] If an organization decides it has legitimate interests that permit the use of video surveillance, all of the findings and the conclusion should be set forth clearly in the LIA; every testing organization needs to retain this document as part of its recordkeeping under applicable privacy laws and regulations.

A related issue is the retention of video used in online/remote proctoring. Since the period of finalizing scores and dealing with scoring challenges can often take months, the controller and its proctoring service provider are likely to need to retain video until that period expires. In the event that review of a video identifies test irregularities involving specific test takers, then further retention may be justified until such time as those issues are resolved.

Accordingly, a 72-hour retention period (e.g., under GDPR and CCPA), is usually not long enough to permit reliance on the video for the legitimate purposes (as articulated in the LIA). If it is not possible for a testing organization to define a retention period that works for all use cases, then the criteria used to determine that period should be determined and recorded in the LIA. In practice video footage should be securely deleted within the shortest period of time that is reasonably practical in the circumstances.

H. Proctor Training and Process Review

The controller needs to execute a written, signed agreement covering data privacy with each processor and sub-processor involved in the use of online/remote proctoring. The controller should also require that the proctoring service provider have a signed written agreement covering data privacy

[3] A testing organization that is considering online/remote proctoring for the first time may use a Data Protection Impact Analysis (DPIA) that is performed where processing of personal information is likely to result in a high risk to a test taker's rights and freedoms. The end goal may be the same as with "in-person" proctoring – to ensure the fairness, security and defensibility of the test or program – but getting there is different. Some organizations may wish to complete a "mini-DPIA" to make a threshold determination of the risk and requirement for a full DPIA. If the outcome of the mini-DPIA is that there is no high risk to the test taker, then a full DPIA should not be necessary.

[4] The European Data Protection Board released final guidelines on the processing of personal information through video devices, which can be accessed here. Although these guidelines do not specifically address online/remote proctoring – and they are not strictly legally binding – the guidelines provide insight into the considerations discussed in this Bulletin. The guidelines also underscore the importance of carefully considering the above and other factors when using online/remote proctoring and working with a vendor that understand the issues.

requirements with each proctor under its control. At a minimum, that agreement should include a legally enforceable confidentiality clause regarding how the proctor is to handle test taker personal information when performing any online/remote proctoring, especially to ensure that such information is not shared with or disclosed to any unauthorized persons. Additionally, the controller should require that the proctoring service provider also has trained (or verified the training of) each proctor in data privacy related to online/remote proctoring.[5]

A final issue for testing organizations/controllers is to identify how the online/remote testing environment needs to be managed. Since proctors normally have no discretion to change standard administration practices, a test program/controller needs to consider what guidance it gives to proctors for everything from handling introductory instructions, to broadband limitations, to new challenges around accommodations, to the need for breaks on a long test, to noise distractions at home – all while ensuring the validity of the test scores.

CONCLUSION

This bulletin contains a discussion of the privacy considerations surrounding the use of online/remote proctoring and how a testing organization controller should evaluate its needs in the selection of vendors. These considerations will better inform the organization about its options in response to the impossibility of in-person testing for an unknown period of time. Clearly, if employers, certification bodies, and institutions of higher education start making important decisions without an assessment score, many high-stakes programs are in jeopardy of becoming irrelevant. Some response is necessary. For example, in response to the shut-down of schools across the nation that typically administer Advanced Placement tests in person, The College Board announced that it will be offering shortened versions of AP examinations for students to take on their computers at home. Similarly, ETS announced that it is allowing students to take the GRE via an internet-based, remote-proctored assessment administration platform.

[5] Controllers, processors, and sub-processors need to keep a record of all personnel trained in data privacy, including the dates on which they were trained. In the future, test proctors may be qualified through an annual certification exam that includes data privacy elements. ATP is currently developing an industry standard for online/remote proctoring jointly with the National College Testing Association that is expected to be available by the end of 2020; NCTA intends to create a certification exam based on the joint standard.

