

601 Pennsylvania Ave., N.W. Suite 900
Washington D.C. 20004
www.testpublishers.org

September 9, 2019

Nikki Eatchel, Scantron
Henrik Skovdahl Hansen, Ph.D., Dansk Psykologisk Forlag
John Kleeman, Questionmark
Rob Pedigo, Pedigo & Associates
Ashok Sarathy, GMAC
Rachel Schoenig, Cornerstone Strategies, LLC
Divyalok Sharma, Pearson VUE
**Cicek Svensson, Cicek Svensson Consulting*
Kimberly Swygert, Ph.D., NBME
Alex Tong, ATA
Alina von Davier, Ph.D., ACT
Linda Waters, Ph.D., Prometric
John Weiner, PSI Services LLC
**Chair*

Chief Executive Officer: *William G. Harris, Ph.D.*
Chief Operating Officer: *Lauren B. Scheib*
General Counsel: *Alan J. Thiemann, Esq.*
Secretary: *Andre Allen, Fifth Theory LLC*
Treasurer: *Amy E. Schmidt, Ph.D., ETS*

BEFORE THE EUROPEAN DATA PROTECTION BOARD

Re: Comments on Guidelines for Video Surveillance

The Association of Test Publishers (“ATP”) submits these comments to express the serious concerns of the testing industry to the **Guidelines 3/2019** document (“the Guidelines”) on non-law enforcement processing of personal data through video devices, as adopted by the European Data Protection Board (“EDPB” or “Board”) on July 10, 2019, and published for public consultation on July 12, 2019. This submission is being made by the required date of September 9, 2019. Further, the ATP fully understands that, as required by GDPR Art. 70(4), the EDPB must make the results of this consultation public, and therefore its submission will be published in its entirety on the EDPB website; there is no personal information in this submission that requires protection by the EDPB.

The ATP is the international trade association for the testing industry, which includes a regional organization for European organizations. The ATP is comprised of hundreds of publishers, sponsors, (i.e., owners of test content, such as certification bodies) and test delivery vendors of tests used in various settings (including healthcare, employment (e.g., employee selection and other HR functions), education (e.g., academic admissions), clinical diagnostic assessment, and certification/ licensure/ credentialing), as well as businesses that provide testing services or administer test programs (“Members”). Since its inception in 1987, the Association has advocated for the use of fair, reliable, and valid assessments, including ensuring the security of test content and test results. Our activities have included providing expertise to and lobbying the US Congress and state legislatures in the United States on proposals affecting the use of testing in employment, as well as representing the industry in regulatory matters and litigation surrounding the use of testing. In providing specific education on the GDPR for its Members in the EU and the US, the ATP has published a “Checklist for EU-US Privacy Shield Registration” (2016) and a “Compliance Guide for the EU General Data Protection Regulation” (2017).

The ATP respects the goals of the Guidelines to ensure that individual privacy is protected as much as possible when video surveillance is used. However, we strongly believe that there are specific circumstances common in the testing industry where video surveillance is both appropriate and necessary, where its use is justified when balanced against the rights of

individual test takers, and where this technology should be allowed within the constraints of the GDPR. Thus, the ATP requests that the Board modify the Guidelines to include the examples presented here, along with explanations clarifying how those examples and proposed edits comport with the GDPR, including for consistency with Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, adopted on April 9, 2019 (the “Online Services Guidelines”).

Many testing events occur in today’s society, which greatly benefit society in general, along with test users and individual test takers. EU citizens are no exception to the vast – and growing – use of assessments by individuals to help themselves to advance personally or professionally. Not considered within these comments is any educational testing in an educational classroom or testing of children of any age, but especially under the age of 16 – those situations are not ones where video surveillance is likely to be used.¹ But as adults, individuals voluntarily submit to testing for many reasons, whether it is to obtain a driver’s license, to learn what motivates them, to identify ways to improve their lives, to understand their academic strengths and weaknesses, to gain admittance to an institution of higher learning or other academic/adult educational program, to seek employment or to gain a promotion once employed, to become licensed/certified in a profession, where a public interest and/or consumer protection motive often exists (e.g., medical, legal, accounting, airline pilot, police, EMT), to become certified in sport/recreation (e.g., flying, scuba) or professionally (e.g., IT certifications in literally thousands of technical skills), and even to learn about their own health (e.g., diagnostic tests) or how to provide lifesaving procedures on others (e.g., CPR). These situations are but a few examples of “high stakes” secure testing (i.e., where the outcome of a test carries a significant consequence for the individual and the test items are kept secure so future test takers do not obtain advance knowledge of them, which invalidates the test results). Testing has become part of our daily lives; individuals generally well understand that testing provides benefits directly or indirectly, by assisting to serve the public health, safety and welfare of the community or society as a whole. Within this context, it is important to note that some testing events in Europe are established and controlled by national or local governments, where public health and safety, or consumer protection goals, as well as ensuring unethical individuals are not given positions of trust, underlie the reason for the test.²

Thus, it is vitally important that any testing program is able to ensure its test administrations are fair to all test takers – in so doing, a testing organization must be able to ensure that an individual who appears on the appointed date and place to take a test is in fact the same individual who is registered to take the test (with or without establishing that s/he is eligible to take the test), and furthermore, that its testing events are adequately monitored to ensure that admittance to the testing location (e.g. secure test center) is controlled and that testing irregularities which may have an adverse impact on every test taker in the room are monitored

¹ However, the ATP is aware that some school admissions testing of minors increasingly is done by computer, where a legitimate interest may involve the use of video surveillance in the future. In all such situations, the ATP would expect that the controller would require a test taker agreement to be signed by the parent, inasmuch as minors do not have legal status to enter into such an agreement.

² The ATP recognizes that where public sector controllers are responsible for the use of audio/video surveillance, the GDPR prevents the use of a legitimate interest. See Para. 23 and Article 6 (1) sentence 2. However, the ATP comments provide a strong argument for the testing organization controller on behalf of the public sector entity to allow the use of audio/video surveillance of individual test takers as a “necessity for the purposes” of the test.

and handled in an appropriate manner).³ Equally important, testing organizations follow the principles of data minimization, including limiting areas of use (not public), limiting the number of people who are monitored, limiting time of surveillance (only during test administration), only accessing the recording to determine if any cheating or IP theft has taken place, and only retaining the record for a necessary period of time (based on the rights of the test taker to challenge test results).

Because of the unique elements of these secure “high stakes” testing programs, the ATP urges the EDPB to distinguish the circumstances surrounding the use of video surveillance to accomplish the controller’s legitimate interest of protecting all individuals -- who take a test and expect the results to be fair and to prevent cheating by some individuals that would have a serious negative impact on individuals who did not cheat – and equally protecting testing programs, who must produce accurate test results that may be relied on without hesitation by governments, certification bodies, employers -- and by individual test takers themselves. We encourage the EDPB to recognize that this analysis establishes the required balancing of the privacy rights of every individual with the rights of the test sponsor and the testing service organization that provides the testing services, as required by the GDPR.

Overview of Concerns

In order to best inform the Board and provide an introduction to the issues specific to testing, the ATP has structured this overview of its specific comments. These topics provide a high-level overview of the issues and positions on those issues on behalf of the testing industry.

Continuing Legitimate Interest: Fundamental to its comments, the ATP requests that the EDPB take notice that testing organizations have a pervasive and continuing need to use audio/video monitoring for the following legitimate purposes: (1) to ensure fairness in testing; (2) to prevent fraud (i.e., cheating) by individuals taking a secure test; and (3) to protect proprietary (and often copyrighted) secure “high stakes” test items from being stolen and illegally distributed by individual test takers. Testing organizations are transparent about their video monitoring usage by providing clear notice in their agreements and reminder notices provided to test takers (e.g., verbally when the test is taken at home), well before the testing event, as well as signage (e.g., posters) at the test site prior to entering the testing room. Only the individuals that are being tested are subject to audio/video monitoring – there is no continuous monitoring, no monitoring of public areas, or of the test takers themselves beyond the test administration process. Tests are administered in private locations (e.g., individuals at home, at a secure testing center or at a central venue). The audio/video recorded data is retained only for necessary periods, which generally is until the tests from a specific event are scored, scores are processed, validated, and reported to individuals, and the period for test taker challenges expires. After the actual test administration, the audio and video recording is generally referenced only to determine if there are testing irregularities or evidence that cheating has taken place, where legal claims have been made, or in response to law enforcement requests.

Test Administration Requirements: The ATP also urges the EDPB to recognize that administration of tests often involves at least two organizations: the sponsor is the owner of the test (e.g., government, certification body, educational institution) who is the data controller that

³ It is important to recognize that in most high stakes tests, the test-taker is expected to answer questions on his/her own, without receiving any assistance from another person or by using reference materials or notes, or having unauthorized access to the Internet.

determines the purposes and uses for collecting and processing personal information;⁴ and the test administration service provider, who is the processor.⁵ When a single service provider is involved, that organization also scores the test and provides score reports to test takers; in some situations the scoring/reporting services are performed by a separate processor. In normal situations, the sponsor contracts with the service provider and spells out the limited use of personal information that is allowed related to obtaining and sharing the outcome of test results with the sponsor; most service providers are forbidden to conduct any direct or indirect marketing to individuals and even emails sent to individuals reminding them of a testing date must be approved by the sponsor.

It is equally important to understand that a test may be printed (paper-based) or delivered in digital form on a computer or similar device (technology-based), although some test sponsors use a combination of both formats. Test sponsors usually make that format decision and will have developed hundreds or even thousands of test items, or contracted to have tests built by an outside assessment developer.⁶ Once the controller and the processor(s) execute a contract, the

⁴ In many cases, the test owner is a non-profit organization, whose primary function is to develop, maintain, and deliver its test(s) related to issuance of a license, certification, or credential. Some of these sponsors often have indirect partnerships with national and/or local regulatory bodies that rely on the integrity of the sponsors' testing program to deliver fair tests and test administrations and ensure that no unqualified individuals are able to obtain licenses, certificates, or credentials.

⁵ Test taker registration may be handled by the controller or the processor, where the individual goes to a website to sign up, establish an account, provide his/her personal information (including in some instances a photograph), and pay for the requested testing services. Most testing organizations will contract with a payment processing entity to handle the collection and processing of payment card information; in these situations, no actual personal payment information is shared with the controller. In most test registration situations, the controller (or processor) uses a formal agreement with each test taker to establish all of the terms and conditions of the testing service, including that the individual is not allowed to photograph or copy any test items, the process by which scores are reported, the right to challenge those scores, the time frame for an individual to be retested, and where appropriate, if video proctoring is used. The individual must give affirmative consent online to these contractual terms and conditions in order to take the test.

⁶ The cost of developing test items for secure "high-stakes" tests, where the items are not intended to be available to anyone because they are used again) is very expensive, often ranging between \$500 and \$1,000 per test question or "item." Some technology-enhanced items (simulations, drag and drop, "hot spot" items) may cost even more. Item development costs are high because they are written and/or reviewed by professionals experienced in their field of expertise, must be determined to be statistically sound, and trialed before actual use in a test that counts. If items are stolen, new items must be developed to replace those them – the test has been compromised and cannot be reused once items have been stolen. Thus, it is vital for a testing organization to protect its intellectual property rights in the test content, and in so doing, to protect integrity of the test results in order to assure fairness for all test takers. A survey of ATP Members conducted in 2018 revealed that over 60% of those organizations responding had to retire items because of any single security breaches to one test or one program, ranging from a modest number of items (20 or fewer) to more than 500 items. *ATP Security Survey Report*, Section 5 Characteristics of Test Security Breaches/Effect of Items and Forms, p. 38 (January 2019) ("2018 ATP Survey Report"). The survey also found that 21% of respondents reported a

determination will be made as to how the test will be administered, whether it will be given to all test takers in a central location (e.g., a test center) or if it will be available to test takers on demand (i.e., allowing an individual to take the test at any time), along with a decision if the test can be taken at any location (e.g., at home or other non-specified location).

Monitoring of Test Takers: Regardless of whether paper-based or technology-based tests are used, or where the test administration takes place, proctoring the test is required to assure standard test administration.⁷ Monitoring, or “proctoring” a test can be performed by live human proctors (on site), and increasingly by video surveillance (live remote or recorded and reviewed later), to increase the ability to effectively monitor all test takers and prevent cheating. Audio/video surveillance, including CCTV, can be used in a central location test center (where hundreds or thousands of individuals take a test at the same time), or video surveillance can be used remotely, where the audio and video recording is reviewed offsite by human monitors, either in real time or after the conclusion of the test session. Remote video surveillance (using the webcam and audio connection through the individual’s computer in real time) is the only option available to monitor individual test takers who take a test at home or in any non-central location (e.g., an office, a school) – such “on demand” testing is available at any time for the convenience of the individual test taker, who does not wish to travel to a central test administration location or where the individual has a disability.

Key Purposes of Surveillance: Audio/video surveillance has become increasingly necessary to ensure the integrity of the test administration process, because it serves several key purposes. First and foremost, the presence of audio/video surveillance in each room in a test center enables the test administration organization to fully monitor each test taker to observe the illegal use of a mobile phone to steal the testing organization’s test items, or the illegal use of devices to cheat in gaining an unfair advantage over other test takers and illegally pass a test to obtain a license or certification that is not fairly earned (e.g., paper cheat sheets, pens/pencils with cameras, glasses with a camera, or ear pieces with a miniaturized microphone to communicate with another person to get answers), as well as to obtain an audio record of any communications between the test taker and the proctor. A human proctor in the room is only able to observe what his/her eyes are focused on at a particular moment in time; when the proctor’s attention is diverted, other test takers may be able to cheat. Equally important, whereas

“high” risk to its program, customer, or brand, from the theft of test items, incurring a cost of between \$50,000 and \$100,000 (or more) (see Section 5/Severity of Breach p. 37).

⁷ Standard test administration is required to assure that everyone who takes a test has the same opportunity to be measured on a test given under the same conditions to achieve fair results. See *Standards for Educational and Psychological Testing* (2014), a set of professional test standards first developed in the 1950s by the American Psychological Association, the American Educational Research Association, and the National Council on Measurement in Education (“Joint Standards”). The Joint Standards have been recognized in many countries around the world; in comparison, the International Test Commission promotes good practice in test construction and use through the development of best practice guidelines. See also, ISO 10667 - - Parts 1 and 2 (2011) Section 5.4 (Note), which requires that “... when administering an assessment to one or more individuals, assessment administrators follow the standardized procedures for the delivery of the assessment and document any deviations from those procedures.” Standard administration requires observing the test administration, to identify any irregularities that may occur (e.g., use of cheating devices, existence of a power failure, medical emergency, disruption of test takers), as well as to protect the test content from being copied and illegally distributed (e.g., infringing the owner’s copyright).

a human proctor provides a subjective view of what is occurring in a testing location, audio/video surveillance provides an objective view of all activities taking place, which protects innocent test takers from the actions of unscrupulous ones, who are intent on stealing test items and/or cheating on the test, as well as allowing an individual who is accused of stealing or cheating to challenge that determination and request a review of the audio/video recording to seek to exonerate himself/herself. Importantly, these recordings are solely for the use of the controller/processor strictly for the purpose of ensuring integrity of the test and kept confidential by the controller and processor” – these recordings are guarded as evidentiary records and are never uploaded to the Internet or social media (e.g., Facebook, YouTube) for public consumption.

Second, the technology enables the test administration organization to verify the individual who shows up to take the test is in fact the person who registered for the test by matching the information obtained at registration (e.g., a photograph uploaded at the time of registration).⁸ This technology provides more accuracy than checking a picture ID, which can be faked. Video surveillance helps prevent the use of “proxy” test takers by cheaters, a practice which has grown to epidemic proportions, as well as helping identify if someone other than the registered individual is trying to enter the test center in order to steal test items.⁹

Remote proctoring: Online (or remote) proctored testing events use audio/video surveillance as the only method to proctor a test session, because there is no live proctor physically present in the testing room; instead, a human proctor observes all of the test takers through a one or more video cameras installed in the testing location.¹⁰ This is a proctoring method that many testing organizations use to ensure fairness during testing, determine if fraudulent activities occurred, and protect proprietary information. The same technology also is used in a home setting of the individual test taker, so no other individuals would be in view of the camera and use is limited to the testing session. For this type of remote testing, the use of video surveillance represents nothing more than requiring the test taker to use the webcam on his/her computer to reveal the test taker’s face and surroundings to verify s/he is the registered test taker and to keep the individual from copying items and/or cheating, and the use of an

⁸ Many testing programs that require an individual to complete a series of required courses or training in order to be eligible to register for and sit for the high stakes test (e.g., licensing, credentialing exam). Thus, it is vital to be able to assure at the location of test administration that the proper person (i.e., who is eligible and registered) is in fact sitting for the test, not a proxy committing fraud on the testing organization.

⁹ In many cases, the theft of test content is perpetrated by profit-driven “test prep” organizations, who recruit and pay individuals to sit for a test in order to steal secure test content so the commercial business can sell the harvested actual items to future test takers, thereby enabling those individuals to cheat. The ATP notes that when a controller’s IP is stolen and illegally distributed (e.g., to a test prep company), who then further distributes or sells the IP, the controller may pursue claims of infringement, giving rise to potential that the audio/video surveillance recordings will be used by law enforcement to prosecute the criminal action.

¹⁰ Even where live proctors are used to establish a more secure environment, most testing organization administering very secure “high stakes” tests elect to use video surveillance that enables recording the session for review afterwards to investigate testing irregularities that pose a pervasive and ongoing threat to testing program integrity, and to have an objective evidentiary record in case challenges (either administrative and/or legal) are made by test takers in that session.

Internet connection so the human proctor can communicate with the test taker (e.g. to provide instruction on the test administration and answer questions before the start of the test). This action is no different than a person's voluntary use of Skype or other method of communicating which displays the individual's face, or an individual going online to play a multi-player video game that records personal information. Moreover, in remote proctoring settings, principles of data minimization are met and there is no continuous monitoring activity beyond the actual testing period. Testing organizations have a legitimate interest to monitor test takers to ensure testing fairness,¹¹ prevent fraud/cheating, and protect proprietary test items.

DPIAs: As noted above, testing organizations only use audio/video monitoring for legitimate purposes -- ensuring fairness in testing, preventing fraud/cheating, and protecting proprietary test items against theft. Indeed, these purposes universally comprise a legitimate basis -- there should be no need for a case-by-case analysis (but see contra. para. 7 and para. 128) because significant historical, country-specific data exists over the past ten years to show that cheating and fraud on exams is both pervasive and an ongoing threat to any testing program's integrity, reputation, and purpose. This data is far more compelling than a specific testing organization's own experiences. Moreover, as stated in the Overview, use of this technology by testing organizations is not systematic; it is limited in time, scope and purpose, and used in a limited space related to specific individuals who have paid to take a particular test. Thus, audio/video monitoring is a critical, objective tool to help ensure a fair and consistent testing administration for all individuals who are taking a specific test. This technology in fact is used to provide a level playing field for all individuals who register to take a specific test (in a central location or at home).

Record Retention: Testing organizations have a legitimate need to retain the video recording of a test session for longer than the "2-3 days" retention period discussed in the Guidelines. First, any test taker has a given number of days to challenge his/her score, which time frame can only commence after the scores are reported, which can occur immediately following the test, or may take months -- this period varies greatly depending on the test program. The recording is only used for investigation of test administration irregularities, for individual score challenges, and for defense of claims by individuals -- not for other purposes. Significantly, test sponsors have a track record of being rigorous in assuring that video recordings are not being used for any marketing purposes -- the use recordings are limited to achieving test security and consistent test administrations.

In submitting these comments, the ATP has identified useful references in the Online Services Guidelines adopted by the Board, see Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (as adopted on April 9, 2019). The ATP also believes that the Video Surveillance Guidelines could be considered to be inconsistent with in some measure the teachings of some elements articulated in the Article 29 Working Party Guidelines on Consent under Regulation 2016/679 ("Guidelines on Consent"), adopted on November 28, 2017, as revised and adopted on April 10, 2018. Where appropriate to our comments, we will reference those other documents and attempt to provide language by which the EDPB may clarify these Guidelines.

¹¹ Another important benefit of remote proctoring is that it allows individuals in remote locations or in developing countries to be able to take an assessment. So, fundamentally, there is overall greater fairness and equity in providing remote-proctored testing.

Comments on Specific Guidelines

1. Introduction [Para. 1]

In pointing out the need for guidance, the EDPB states that video surveillance technology often limits an individual's "anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed." As compelling as that statement may seem at first blush, it ignores the reality of the use of video surveillance in testing, where the technology ensures that the individual who has registered for the testing service is not supposed to be anonymous. Indeed, each test taker must be verified for the protection of all test takers in a testing event, as well to protect the testing program. Any testing program is at risk of being damaged monetarily or having its reputation and the integrity undermined if some individuals can get away with cheating. Moreover, unqualified test takers who pass the test via cheating may pose a serious threat to public safety and welfare, and could result in unethical persons (who cheat on the test) being placed in a position of public or corporate trust. Broadly, then, individuals seeking a publicly-recognized and/or professionally-mandated certification or government-issued license automatically forego their anonymity, at least in the context of the testing process.

Given these factors, the ATP requests that the EDPB clarify the existence of some limitations to its statement by adding the following language to the sentence, "in settings where the GDPR prohibits it."

2. Introduction [Para. 2]

The EDPB expresses concern that the use of video surveillance must avoid any "misuse for totally different and – to the data subject – unexpected purposes (e.g. marketing purpose, employee performance monitoring etc.)." As discussed in the Overview, testing organizations affirmatively protect against any misuse beyond the legitimate purposes explained to each test taker (in the test taker agreement) and do not have a history of abusing the legitimate purposes for which video surveillance is used: ensure testing fairness, prevent fraud and protect proprietary test items.¹² To the contrary, testing organizations have historically been transparent about their video monitoring by providing clear notices of such monitoring, and by providing extensive appeal procedures for individual test takers when testing irregularities are suspected and video recordings may be relied upon.

To provide adequate consideration to situations where the controller and processor have taken affirmative steps contractually to prevent the use of audio/video surveillance data from being used for any "marketing" (or "employee performance") purposes, the ATP requests the EDPB clarify this paragraph by adding the following sentence following the first sentence: "When the controller has taken appropriate steps to guarantee through a legal contract that there will be no undisclosed purposes for the use of data subjects' personal information, individuals' consent may be deemed sufficient."

¹² Similarly, audio/video surveillance of employees is consistent with the testing purposes (see Sections 6 - 8) and is limited to the testing session. Although the controller may be the employer, an independent testing organization is often the controller. In either case, any use of surveillance is intended to support the fair testing purposes and benefit the employee (e.g., promotion, award of certificate/credential).

3. Introduction [Para. 4]

Users of video surveillance products should be aware that it is possible the technology to contain vulnerabilities that hackers can exploit. The last sentence of this paragraph should be modified to read as follows: “data controllers must also ensure that personal data processing derived from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided, as well as to monitor it for any security vulnerabilities that may occur.” The ATP also believes this language is consistent with the Section on Technical Measures (see Paras. 129-131), which we also endorse.

4. Introduction [Para. 5]

As applicable to the testing industry, this paragraph is overly broad in its contention that “Video surveillance is not by default a necessity when there are other means to achieve the underlying purpose.” As the ATP has shown (see Overview), in testing today, the use of video surveillance provides unique benefits that are not met by the use of human proctors. Indeed, as stated in Recital 47, “The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.” (See also Section 7 of these comments). Consequently, a new sentence should be added at the end of this paragraph, to read as follows: “Nevertheless, using the required balancing analysis, some users of video surveillance may be able to demonstrate that video surveillance achieves significant benefits for both individuals and controllers, including the prevention of fraud, that cannot be matched by other means.”

5. Section 2.3, Household Exemption [Paras. 11-14]

As noted in Para. 11, the household exemption can cover personal online activities. Although we understand that the exemption should be narrowly construed, the ATP contends that audio/video surveillance for “on demand” testing by an individual in his/her home does not involve “the constant recording and storage of personal data” or cover, “even partially, a public space and is accordingly directed outwards from the private setting.” (citing the ECJ Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*, 11 December 2014, para. 33). Moreover, the provision of on demand testing services constitutes an “online service” for the purposes of the Online Services Guidelines. Indeed, as noted in the Online Services Guidelines [para. 2], “If the specific processing is part and parcel of delivery of the requested service, it is in the interests of both parties to process that data, as otherwise the service could not be provided and the contract could not be performed.”¹³ Although the ATP is mindful of the language of Recital 18, the Board should consider that the ability to take a test at home is for the convenience of the individual (to avoid traveling many miles to a secure brick and mortar location, or to accommodate a person’s disability). Considering all of these factors (see para. 13), it seems reasonable that the agreement by the test taker to use his/her home computer for the test

¹³ While the “commercial” nature of this relationship might suggest the exemption should not apply, the nature of the data collected is for the benefit of the individual. Indeed, the testing scenario is similar to other personal online services where the household exemption would also logically apply (e.g., online commercial gaming where personal information, including voice and/or audio information, is shared with other players and with the game provider, to provide entertainment value to the individual). This testing information is limited and well protected, even with review by a human proctor, more so than that with online household personal assistants.

administration, along with the limited scope of the audio-video activity, qualifies surveillance usage for at home testing to be outside the scope of the GDPR.

Based on the above, the Board should include following example in Para. 14:

“Example: An individual has registered to take a test at home on his/her own computer. The testing organization responsible for downloading the test items and monitoring the test administration requires that only the test taker is allowed in the room and asks the individual to scan the room before the test begins to make sure the individual does not have materials to cheat on the test. The individual’s computer camera records the test administration, which is shared online with the test administration vendor so its human monitors can ensure that only the test taker is present; also, the test taker and the proctor are connected via Internet so the proctor can communicate with the test taker. Since no other persons are recorded and the test taker has chosen to use his own computer for the purpose of taking the test at home for his convenience, this use of audio/video surveillance would fall under the household exemption.”

6. Lawfulness of Processing [Paras. 15-16]

The Guidelines (Para. 15) highlight that Article 5 (1)(b) requires that the controller state with specificity the purposes of any processing and that data subjects must be informed of the purpose(s) of the processing in accordance with Article 13. The ATP reiterates its position that the use of audio/video surveillance by testing organizations serves three clearly identified legitimate purposes, to: (1) ensure testing fairness for all test takers who take a particular test; (2) prevent fraud/cheating on the test, to ensure that every test takers score is accurate; and (3) protect proprietary test items from being stolen. These purposes are effectively communicated by the testing organization to each test taker in a legally binding agreement at registration (and often repeated again before the start of the test administration, which we contend should be deemed to meet the requirements of Article 6(1)(f) (legitimate interest) (Para. 16). Signage and posters are also used at test centers or for paper test administrations; screen notices are used on testing computers, either at home or in a secure test center. Also, as stated in Para. 16, in exceptional cases Article 6(1)(a) (consent) may be used as a legal basis by the controller.

However, the Board should equally recognize that consent to capture test takers’ voices and images is “necessary for the provision of the service” because without the ability to fully proctor the test, some of the purposes may not be accomplished. But according to Opinion 06/2014 of WP29, the term “necessary for the performance of a contract” must be interpreted strictly, and processing must be necessary to fulfill the contract with each individual data subject – which occurs when the controller/processor uses a test taker agreement. There needs to be a direct and objective link between the processing of the data and the purposes of the execution of the contract, but if a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the appropriate lawful basis. See 2017 Guidelines on Consent p.8. While the ATP strongly believes that, under the 2017 Consent Guidelines, audio/video surveillance is “necessary for the performance of the contract.” And when the controller provides a test taker agreement with clear, transparent language to communicate the purposes for the use of audio/video surveillance, the appropriate lawful basis is then Article 6(1)(b) (contract). The ATP contends that, in most cases, the data captured in video surveillance of a test taker should not be considered special categories of data, but if and when it is, it would seem reasonable where a test has legal implications or a dispute could arise because of a test, that

Article 9(2)(f) should be applicable in these situations.¹⁴ These positions should be articulated in the Guidelines, whether in text or an example (see Comment 8 below).

7. Section 3.1.1, Existence of Legitimate Interest [Paras. 18-21]

The Guidelines call out to the need for the controller, itself or its processor, to demonstrate that their legitimate interest (see Comment #6 above) in using audio/video surveillance overrides the fundamental rights and freedoms of the data subjects (i.e., the test takers at each specific testing event), as required by Article 6(1)(f). As mentioned in the Overview, the ATP contends that existence of legitimate interest for the use of this technology is the principal lawful basis – as explained later in these comments, the use may also be necessary for the purposes of testing and, in certain setting, authorized by contractual rights. While these lawful bases are independent of each other, collectively, they assure that testing organizations are able to provide a fair opportunity for all individuals that is free from cheating by some test takers, and the protection of test items (controller’s or processor’s IP).¹⁵ In reality, refusal by an individual test taker to be videotaped under the guise of privacy rights is tantamount to saying “allow me to have the opportunity to cheat” – the individual represents a threat to steal test items or cheat on the test and create an unfair testing situation. Thus, no single individual’s privacy rights should be allowed to outweigh the collective legitimate rights of all other test takers in the testing session (all test takers who have no intention of stealing or cheating) – and equally the public interest and the corresponding legitimate interests of the controller/processor. Moreover, the audio/video recordings protect both the individual test taker and the controller/processor because the video recording can be used as an objective tool by both the controller (and the individual if requested) to determine that cheating or a testing irregularity took place.

In recognition of this balanced view of the existing legitimate interests of the controller/processor and a shared public interest supporting the collective rights of all other test takers to be able to take the test in an environment free from cheating, the ATP requests the Board to add the following example in para. 21:

“Example: A test sponsor wants its test administration vendor to install a video surveillance system at its secure test center to monitor every test taker to ensure testing fairness by making sure they don’t steal test items or cheat on the test. The sponsor can also show evidence demonstrating that it has experienced a significant number of test takers in past years try to steal its test items by secretly bringing a mobile phone or miniature concealed recording device into the test room for the illicit purpose of photographing or video-recording the computer screen, and that a high number of test takers have tried to cheat by using various devices to enable them improperly to obtain answers to the test items. The controller/processor can show that video surveillance has been demonstrated to promote fairness in testing by significantly reducing

¹⁴ It seems to the ATP that Article 9(2)(f) would apply the collection of video surveillance information, inasmuch as the controller should be able to assert the existence of a “legal dispute” (or possibly a full blown administrative or judicial challenge) that would override an individual objection. See discussion in Section 13 on the right to object and the right to erasure.

¹⁵ Failure by the testing organization to prevent cheating also may result in harm to the public at large by enabling individuals to obtain illegitimate professional certifications/licenses (e.g., healthcare, stockbrokers, real estate agents) that could jeopardize the health and safety of the public, or consumer protection. Where legitimate interest is the lawful basis, the test administrator service provider handling the audio/video surveillance would be subject to processor requirements under Article 28.

both item theft and cheating. This documentation is strong evidence showing the existence of a legitimate interest.”

Even beyond the legitimate interests of the controller, a public interest exists related to today’s testing scope and environment (see Article 6(1)(e)). In fact, a number of specific prevailing public interests can be identified that support the use of audio/video surveillance during secure “high stakes” tests, including but not limited to:

- deterrence and/or prevention of proxy testers;
- deterrence and/or prevention of cheating;
- deterrence and/or prevention of test item mining/theft;
- deterrence and/or prevention of collusion between test takers and/or between a test taker and test delivery staff to alter the results of an test through unauthorized assistance; and
- deterrence and/or prevention of misconduct of test takers that is prohibited by the controller’s requirements and/or by test center regulations.

As explained earlier, the public interest ensures that individuals who seek and obtain many different licenses and certifications are required to earn them on their individual merits, to demonstrate they each possess the knowledge and skills necessary to work in those professions, and that they do so on their own, with assistance or cheating. To fail to recognize these public interests is to facilitate fraud in the system and permit unauthorized individuals to work without regard for safety and health risks to all citizens and/or where consumer protection is jeopardized.

The Board previously addressed topic this in the Guidelines for Online Services, stating generally that “processing for fraud prevention purposes may involve monitoring and profiling customer” but opining that “such processing is likely to go beyond what is objectively necessary for the performance of a contract with a data subject.” (see Section 3.2 [Para. 47]. As the Board recognized, “such processing could however still be lawful under another basis in Article 6, such as legal obligation or legitimate interests.” The ATP strongly encourages the Board to provide further guidance in Para. 47, by finding that, “The prevention of fraud by the use of video surveillance is in the public interest, which may be further supported by the legitimate interests of a controller.” This finding is consistent with Recital 47 (“The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.”)

In order to clarify its guidance on the relationship of audio/video surveillance to fraud in testing, the ATP requests the Board to add another example to Para. 42, to read as follows:

“Example: Individual A wants to become a doctor but has not been able to earn high enough score on the medical entrance exam to be accepted by an accredited university program. Individual A hires Individual B to take the medical entrance exam in Individual A’s name. Individual B passes the medical entrance exam with a very high score under Individual A’s name, and Individual A is set for acceptance to a prestigious medical program. Several months after the scores are issued, the testing organization that issues medical exam credentials becomes aware that a well-known proxy tester may have tested in place of Individual A, and requires review of the video surveillance footage of “Individual A’s” assessment experience to validate the identity of the actual test taker. This use of video surveillance is justified as a matter of public interest in preventing fraud, supported by the legitimate interest of the testing organization.”

8. Section 3.1.2, Necessity of processing [Paras. 24-29].

The Guidelines seem to assert (Para. 24) that “data minimization” (see Article 5(1)(c)) requires the controller reasonably to fulfill its purposes for processing “by other means which are less intrusive to the fundamental rights and freedoms of the data subject.” The Guidelines also state (Para. 26) that, “Usually a surveillance system operating at night-time as well as outside the regular working hours will meet the needs of the controller to prevent any dangers to his property” -- a conclusion that clearly does not meet the legitimate purposes of testing organizations. The Guidelines (Para. 25) give an example of an alternative to video surveillance of having a security guard patrol the premises. As already noted, in testing, a human proctor may miss some actions that the video surveillance catches.¹⁶ As such, audio and video surveillance, conducted only during a testing session, is necessary for more efficient monitoring, which will better ensure a fairer test administration process for all test takers.

Equally difficult to resolve is the Board’s apparent guidance (Paras. 24-25) that the controller/processor is required to offer every individual test taker the option of taking the test with only a human proctor or with audio-video surveillance. As discussed earlier, there are advantages in scope and accuracy of evidence obtained from the use of audio-video surveillance that can be matched by human proctors, which establishes a legitimate interest. Moreover, it would not be reasonable to require every testing organization to operate in the same secure location both testing rooms with human proctors and other rooms using video surveillance. The costs of such inefficient operations are not feasible or justified.¹⁷ Equally persuasive is the dilemma confronting every testing organization of overcoming the strong suspicion that any test taker who chose to be tested with human proctors did so in order to enhance his/her opportunity to cheat or steal test items.

Finally, testing organizations may effectively apply the principle of data minimization to their operations and yet reasonably conclude that there is no “less intrusive” means to accomplish its purposes than audio/video surveillance as a justified “necessity of processing.” The Board should add a new sentence at the end of in Para. 24, to read as follows: “Video surveillance measures may be chosen for the purpose of the processing when less intrusive alternatives do not reasonably fulfill the purposes of processing.”

Consistent with these comments, the ATP requests that another example should be added to Para. 28, to read as follows:

“Example: A testing organization wants to protect its test administration against fraud and theft of its IP so that every test taker has a fair testing opportunity. It strategically places surveillance cameras only to film actions at the check in desk and in the rooms where the test is administered. There are no cameras elsewhere in the premises itself, nor any facing outward to any public spaces because those are not necessary. Only scheduled test takers and scheduled test delivery

¹⁶ Finally, the Guidelines (Para. 29) correctly point out that, “If for example the purpose of video surveillance is the preservation of evidence, real-time methods are usually not suitable.” This, or a similar statement, should be incorporated into earlier paragraphs of this section of the Guidelines.

¹⁷ For many “high stakes” tests that use video-surveillance for security, the test and the test administration procedures are identical throughout the world. Changing the administration to allow optional proctoring would require a complete re-validation of the standardized conditions for testing, and destroy the global comparability of testing in Europe.

staff are permitted in the secure test center (i.e., no guests are permitted). This is an appropriately limited use of video surveillance to prevent fraud.”

9. Section 3.1.3.1 Data Subjects’ Reasonable Expectations [Paras. 35 - 38]

The ATP agrees with the general principle in this section of the Guidelines, namely, that a data subject’s reasonable expectations of privacy should be taken into account. Nevertheless, as shown in these comments, the great majority of testing organizations regularly provide individuals who register to take a test with an agreement that clearly indicates all of the terms and conditions related to the testing event – where video surveillance is going to be used, that fact is explicitly stated in the agreement, along with the explicit purposes for the surveillance. Accordingly, in such circumstances, test takers cannot claim surprise or that being video-taped is unexpected, inasmuch as they are provided with advance notice in plain language about the use of audio and video monitoring during the testing session.

Accordingly, the ATP requests the Board to include another example in Para. 38, to read as follows:

Example: When data subjects sign up to take a test and are explicitly told in the test taker agreement that they will be videotaped during the test administration, individuals should expect to be monitored.

10. Section 3.3, Consent (Article 6(1)(a)) [Paras. 42-46]

Although the existence of legitimate purposes is likely the most compelling basis for a testing organization’s decision to use audio/video surveillance, the Board should recognize that in many instances the testing organization also establishes a contractual relationship with the individual test taker by way of a test taker agreement. This type of agreement contains the legal terms and conditions under which an individual registers and receives the testing services, especially ensuring the testing organization is able to document its legitimate interests in securing its IP while providing a fair and standardized environment for all test takers so that everyone takes the test on a level playing field. Such an agreement is usually provided to all individuals on the registration website, which must be looked at before giving affirmative consent.¹⁸

Accordingly, when the test taker agreement contains explicit notice in clear and plain language that audio/video surveillance will be used (either as part of the “on demand” testing at home or at a secure test center), the individual is given notice weeks (or sometimes months) before the actual test session date. As previously discussed (see Section 6), in testing the consent to capture a test taker’s image is “necessary for the provision of the service” – thus, the

¹⁸ A testing organization’s registration website is usually set up so that the individual must scroll through the entire test taker agreement (and privacy policy) before positively indicating agreeing to abide by the terms and conditions, including giving explicit consent, which action is then followed by the individual checking out his/her account by paying the associated testing fee. (footnote continued from previous page) Thus, there are at least two separate affirmative actions required of an individual in the process of giving consent and establishing the contractual relationship, including an express consent for the audio/video surveillance. Many testing organizations separately repeat the process of requiring obtaining a second affirmative consent on the same test taker agreement at the time of test delivery. Having two separate agreements signed by the test taker provides additional evidentiary support in a court of law.

appropriate lawful basis could then be Article 6(1)(b) (contract).¹⁹ Even though it may not be the primary basis for using audio/video surveillance, the Board should understand that in obtaining the online contractual agreement to take the test, the individual also gives his/her explicit consent to the use of audio/video surveillance.²⁰

The ATP notes with interest the example in Nov. 2017 Art 29 WG Guidelines (p. 6) Guidelines on Consent, which highlights an example where the request for consent related to a mobile app for photo editing services required an activation of GPS locationing and behavioral advertising. The Guidelines on Consent example explains that, “Neither geolocalisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.” By comparison, consent for audio-video surveillance is directly related to the delivery of the purchased testing services and, as shown, is inherently necessary for the provision of the service. The ATP requests that these Guidelines cover the same type of situation to avoid confusion by including an example in Para. 45, to read as follows:

“Example: A legal agreement signed by the test taker with the testing organization, as well as entering a testing room clearly marked for video surveillance, are clear affirmative actions that constitute explicit consent. All of the individuals in the testing room share the same objective (i.e., to take the test they registered and paid for) and there are no other unknown who will be recorded. Advance knowledge of the use of video surveillance has been given to each test taker, by which they each have agreed to be recorded by the testing organization as a means of fairly treating each test taker in administering the test against some who might cheat and protecting the testing organization’s IP. In these conditions, even if the video surveillance identifies individual test takers, explicit consent has been given.”

11. Section 5.1, Processing of Biometric Data [Paras.72-85]

The Guidelines draw significant attention to issues surrounding the processing of biometric data. While the ATP understands the general apprehension, we are concerned that the fundamental principles have gotten lost. For example, the Board states (Para. 85), that, “when the biometric processing is used for authentication purpose, the data controller must offer an alternative solution that does not involve biometric processing – without restraints or additional cost for the data subject.” Moreover, the Guidelines state (Para. 76) that explicit consent must be obtained for all biometric data processing.

These statements should be clarified, for at least two reasons. First, the use of video surveillance by testing organizations does not disclose personal biometric information in each

¹⁹ The Board has previously determined that, “Article 6(1)(b) GDPR provides a lawful basis for the processing of personal data to the extent that ‘processing is necessary for the performance of a contract’ to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This supports the freedom to conduct a business, which is guaranteed by Article 16 of the Charter, and reflects the fact that sometimes the contractual obligations towards the data subject cannot be performed without the data subject providing certain personal data. If the specific processing is part and parcel of delivery of the requested service, it is in the interests of both parties to process that data, as otherwise the service could not be provided and the contract could not be performed.” See Online Services Guidelines [Para. 2].

and every circumstance. The ATP submits that processing of photographs and/or video recordings cannot be considered to be systematic processing of special categories of personal data – instead, these uses are covered by the definition of biometric data only when a video recording is “processed **through a specific technical means** allowing the unique identification or authentication of a natural person” (bold in original, see definition in Para. 75).

Therefore, if a video recording is simply reviewed by a person, the ATP submits that this is not an analysis conducted “through a specific technical means” (i.e., automated analysis, such as facial recognition). This use of the video recording is no different than someone physically checking an individual’s ID (i.e., to make sure it matches the photograph uploaded by the test taker in the online registration) – there simply is no technical processing performed.

Next, because no biometric processing is involved, the ATP reiterates that the use of video surveillance is allowable as “legitimate interest,” Para. 73, quoting Article 4.14 and referencing Recital 51 – this factor is dispositive (“The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual.”).²¹ Finally, the Board’s approach seems more restrictive than the Article 29WP Guidelines on consent, especially the statement that non-surveillance option must be available to the test taker “without restraints or additional costs.” For example, a testing organization could give a test taker the option of taking the test in a different test center that does not use video surveillance – but that obviously would most likely entail some restraint of the test taker and potentially additional costs. In other situations, the test taker who claims a disability may be offered the opportunity to take the test at home, but that option would require the use of audio/video surveillance to ensure the legitimate interests of the controller are met.

Assuming the Board agrees with this interpretation, the ATP requests that the last sentence of Para. 73 of the Guidelines should be clarified to read as follows: “The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed, which does not include human reviews, in order to contribute to the identification of an individual.”

12. Sharing Video Footage with Third Parties [Para. 48-54]

As discussed earlier, the testing organization controller and test administration vendor processor have a clear legal relationship in the handling of personal information of test takers, including audio/video recordings made during any test administration. Usually, the processor is responsible for conducting the surveillance, performing any real time monitoring of the recording(s) from a secure test center or a home/office computer. If any anomaly is noted, the recordings are reviewed in making a determination about whether any individual or individuals were engaged in theft of items or cheating on the test. In some instances, if a forensic investigation is needed to make a more sophisticated analysis of the recording(s), a third party analyst may be contracted to assist in evaluating the recordings to decide whether to invalidate any individual’s test score or to withhold releasing a score report pending further analysis. Any sharing of the audio/video recordings with such third party is expressly limited to the same

²¹ Explicit consent may be demonstrated in many ways. The GDPR does not prescribe written and signed statements in all circumstances that require valid explicit consent. For example, in the digital or online context (e.g., online test registration), a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature.

purpose as the making of recording in the first place -- to ensure the fairness of the testing event for all test takers and to protect the controller's IP.²²

Based on this information, the ATP requests the inclusion of the following example in Para. 52:

“Example: Video surveillance is installed in the testing rooms at a test center for the purpose of capturing a record of attempts at theft of the test IP and any instances of cheating by test takers in the room. Two incidents are captured on video, one of test taker using a cell phone and snapping pictures of the computer screen and another of test taker secretly pulling out a piece of paper and using it to answer questions. In this case, transferring the recordings to a third party for digital analysis of the acts to determine if those individuals' test scores should be invalidated is for the same purpose as the installation of the video surveillance.”²³

13. Section 6.2, Rights to Erase and to Object [Paras. 98-107]

Video surveillance is an integral part of the testing process and is not optional – it is only possible, consistent with the legitimate interests of the controller, to take many “high stakes” tests where security includes the use of audio/video surveillance. To the extent the Guidelines discuss the right of the individual to object to the surveillance and/or the right to erase the recording, the ATP is most concerned about that an unscrupulous individual would use this right to object and then engage in cheating. In these limited circumstances, we believe that the testing organization has a legitimate interest to monitor only the test takers, and that this is a compelling interest that overrides the individual's objection. And an equally strong public interest exists in preventing fraud by test takers, which would be exacerbated if individuals are permitted to object to the use of video surveillance, especially after being informed of its use in the test taker agreement.

Generally, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent -- and in accordance with the GDPR -- remain lawful. Moreover, each separate processing activity can be based on more than one lawful basis (e.g. customer data collection to process the contract may be based on contract performance, but marketing activities are based on consent). Hence, a withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject if the individual withdraws consent. The controller would rely on the lawful basis of contract performance to continue the contract.²⁴ This

²² In line with the concept of purpose limitation (see Article 5(1)(b) and Recital 32), consent may cover different test operations, as long as these operations serve the same purpose (i.e., there is “compatibility of purposes.” See Online Services Guidelines, (p.12).

²³ Article 22 requirements for AI may apply to the use of audio-video surveillance. However, the Board should recognize that no AI issue exists when the audio/video recordings are reviewed by humans, to analyze what is seen/heard on the recording in order to make a decision about how to report/invalidate an individual test taker's score.

²⁴ A request to erase such a record could be denied by the controller if the legitimate purposes for the video are still ongoing (unless consent was the only lawful basis). Allowing an individual to request erasure of the very evidence documenting the individual's actions by which controller is able establish the test taker was cheating would obviously be inconsistent with the controller's legitimate interests.

problem is particularly severe in an instance when an individual has already started taking a test and then wants to withdraw consent. In many of these situations, a test taker has already seen some of the test items, which could already have provided an opportunity for theft of items. At a minimum, the audio/video recording is expected to be retained for review (see Section 14), to assist the testing organization in determining whether to treat the test as taken (and proceed to score it), to invalidate it, or to permit a future retest in accordance with the test taker agreement. As such, withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the test taker, or the consent expressly given prior to beginning the test.

Based on these concerns, the ATP notes that the example in Para. 107 is based on facts, circumstances, and issues, that are reasonably close to those raised here. Accordingly, the ATP requests that the Board add a note to Para. 107, to read as follows: “This example similarly applies to issues in the use of video surveillance in the testing industry, where the existence of a legitimate interest justifies a testing organization rejecting a request for erasure “with the explanation that the footage stored is needed due to an ongoing internal investigation, thereby having compelling legitimate grounds to continue processing the personal data.”

14. Section 8, Storage and Retention [Paras. 118- 120]

The Guidelines suggest that a reasonable retention period is 72-hours (other current EU laws set retention at anywhere from 24-hours to 30-days). The ATP submits there are compelling reasons to retain surveillance recordings of secure test sessions for the duration of the “purpose for which the recording was collected.” This extended retention accounts at least for the time period that it takes to score/return test results and/or covers any applicable appeal processes and time periods granted to test takers, as follows:²⁵

1. Video recordings are retained for a limited, pre-defined period after the test session in case there is any analysis needed to determine if an anomaly (e.g., cheating or theft of test content) took place.
2. In the case of an anomaly, the video recording may be retained for longer for possible use in initiating and/or defending legal claims (administratively or in court).

Consequently, testing organization retain video records for a reasonable period after the test session in case they must be analyzed to determine if an anomaly that could be cheating (or IP theft) took place. Significantly, such analysis requires human intervention. Compliance with Article. 22 requires that there is no automated decision making associated with such physical reviews. The following example should be added to Para. 120, to read as follows:

“Example: A testing organization normal process takes 15 days to receive and score exam results received from its test administration vendor. It normally takes another 5-10 business days to publish results to all the test takers from that administration. During this time the testing organization is also reviewing all exam irregularity reports received from its test administration vendor (e.g. the entity that provided the proctors), and has the discretion to overturn any passing scores it deems were achieved through fraud (e.g., cheating, dishonesty). Review of video surveillance footage of that test session in tandem with such irregularity reports is essential to confirm and/or reject the reports. Under the test taker agreement, a test taker whose passing test

²⁵ Data retention will always be subject to the provisions of Article 5, but see the discussion in Paragraph 13 (infra. at pages 19-20) regarding erasure.

score is overturned through this process has 6 months to appeal the decision. Throughout this time, and thereafter for the extent that the appeal continues or is escalated to litigation, the video recording related to that test taker's test session will be essential to the testing organization's legal defense of the appropriateness of its determination with respect to the test results. Under these conditions, retention of the specific audio/video surveillance recordings pertaining to this test taker is appropriate."

15. Section 9.3.1, Organisational measures [Para. 128]

The Guidelines suggest a list of factors covering different organizational measures that should be considered by a controller that uses video surveillance (see Para. 128). The ATP believes these factors, with some minor editing based on the context of usage by testing organization, are reasonable and that it would be prudent to follow them. Accordingly, the ATP generally endorses the inclusion of such factors.

16. Section 9.3.2, Technical Measures [Paras. 125, 129—131]

The Guidelines address digital equipment, software technical issues, especially system security, physical security, data security, and access controls. The Board comments that, in many ways, these measures are shared in common with all IT systems. The ATP agrees with the Board's analysis and endorses these paragraphs.

17. Section 10, Data Protection Impact Assessment [Paras. 132-134]

The Guidelines state (Para. 133) that, "it is reasonable to assume that many cases of video surveillance will require a DPIA." It advises controllers to determine whether such an assessment is required and conduct it, if necessary. As explained in the Overview (infra. at p. 7), the ATP believes that there is "no need for a case-by-case analysis because significant historical, country-specific data exists over the past ten years to show that cheating and fraud on exams is both pervasive and an ongoing threat to any testing program's legitimate purposes, as well as its reputation and integrity.

For this reason, we request that testing organizations with a legitimate interest as noted are not subject to mandatory DPIAs. Instead, the ATP requests the Board approve a common DPIA based on industry-wide, global experiences covering the use of audio/video surveillance in the testing industry. Such a generic DPIA would obviate the need for each testing organization to focus on the international, historical statistics in setting out the impact of video surveillance. Beyond use of a common DPIA, if test-specific data is available to each specific testing organization, that information could easily be added on top of the generic statement. The value of adopting a common DPIA is that it would avoid (or at least greatly reduce) varying substantive decisions by national Data Protection Authorities and provide more certainty for the testing industry on this important issue. The ATP would be willing to provide assistance in drafting the common language based on the eventual final Guidelines.

CONCLUSION

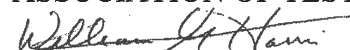
On behalf of the international testing industry, the ATP has provided comments on proposed modifications of the Guidelines, especially the addition of examples specifically dealing with issues surrounding the use of video surveillance by testing organizations under the GDPR. In summary of our positions:

1. There are compelling, legitimate reasons for the use of video surveillance in testing, even if a human proctor is physically present in the testing location. The use of audio/video surveillance will benefit test users, society in general, and the individual test taker as discussed in these comments.
2. In general, when a testing organization is not capturing special data, the usual lawful basis for video surveillance is legitimate interest, the bases for which are documented in these comments. For the average testing organization, legitimate interest provides an appropriate basis for the use of audio/video surveillance in the limited context described in these comments. While a controller will need to document its legitimate interest, that exercise should be routine; the ATP requests that the Board approve a common DPIA specific to testing industry statistics.
3. There are limited cases (e.g. public bodies) where legitimate interest cannot be used, in which case the existence of a contract with a data subject or explicit consent would be the appropriate lawful basis for processing.
4. In most cases, video surveillance data from monitoring test takers is not “special” data because it is not processed **through a specific technical means**. However if biometric technologies are used for uniquely identifying a person (e.g., characteristics, behaviors), explicit consent must be obtained, after providing clear and plain language notices. For those situations in testing, video surveillance is necessary for provision of the service (since otherwise the test is less valid as people might cheat and undermines both public interest considerations and the legitimate interests of the testing organizations).

Thank you for your attention to the important issues about the application of the Guidelines to the testing industry. The ATP is available to answer any questions the Board may have in response.

Sincerely,

ASSOCIATION OF TEST PUBLISHERS



William G. Harris, Ph.D.

CEO



Alan J. Thiemann

General Counsel

John Kleeman

Member of the Board of Directors (representing the European ATP)

Co-Chair, International Privacy Subcommittee, Test Security Committee