IEEE SA
STANDARDS ASSOCIATION

IEEE SA WHITE PAPER

IEEE SA 3D BODY PROCESSING
INDUSTRY CONNECTIONS

SUMMARY AND RECOMMENDED ACTIONS FOR COMMUNICATIONS, SECURITY, PRIVACY, AND TRUST (CSPT) [IEEE P3141]

IEEE

Authored by

Marco Hernandez
National Institute of Information & Communications Technology, Japan

Stephen Hopkins, IEEE Senior Member
Computer Help, USA

Tunmin (Catherine) Jai
Texas Tech University, USA

Randy K. Rannow
Silverdraft Supercomputing, LLC, USA

John Schulz
Luminary Pie VR—Tools & Content Design, USA

Acknowledgment

The authors appreciate the feedback from the IEEE 3D Body Processing Industry Connections (3DBP IC) group and Fred McDonald for preliminary editing this white paper.

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

PDF: STDVA24942 978-1-5044-7955-4

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association ("IEEE SA") publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE SA OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder.

This Work is published with the understanding that IEEE and the IEEE SA Industry Connections activity members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

SUMMARY AND RECOMMENDED ACTIONS FOR COMMUNICATIONS, SECURITY, PRIVACY, AND TRUST (CSPT) [IEEE P3141]

ABSTRACT

3D scanning is a process that captures the three-dimensional attributes of an object and includes surface texture and spectral content. 3D scanners have become a critical tool for shortening product development and manufacturing time. The ongoing technological advancements in terms of portability, scanning range, and image quality have opened new application areas for 3D scanning. However, 3D scanning appears to be primarily dependent on users. Innovation in technology and application software, as well as growing and diverse connectivity, are leading 3D scanners to become a more integral element in the overall value chain. This notwithstanding, interoperability, data security and privacy, quality, portability, and trustworthiness are opportunities to be realized. The intent of this white paper is to highlight areas of opportunity for standard development organizations, specifically the IEEE P3141 Working Group, to focus on and further enable broad market use for the various sectors and users.

1. INTRODUCTION

Broadly speaking, the 3D Body Processing (3D BP) Industry Connection (IC) Communications, Security, Privacy, and Trust (CSPT) group investigated the system representative of the 3D BP ecosystem, which consists of individual scanners that may interoperate using proprietary networks or existing LAN/WAN infrastructure for the purpose of scanning people and allowing individuals to use and share scanned data, in a ubiquitous manner. The 3D BP ecosystem is complex and may be difficult to capture in its entirety, due to the vastness of possibilities, especially considering the ongoing evolution of solutions and potential applications.

3D BP is creating numerous opportunities for engineering and science, as well as users and equipment vendors. The success of 3D BP may depend strongly on standardization to enable communication, security, and privacy, in a trusted environment, as well as further enable interoperability, compatibility, reliability, and effective operation on a global scale. Recognizing the value of 3D BP and the benefits this technological innovation brings to the public, the 3D BP IC group has investigated the ecosystem that may support 3D BP and is forwarding the findings and providing recommendations to the IEEE P3141 Working Group (WG) to help enable the development of a standard to foster broad market acceptance, an environment necessary for a vibrant and evolving 3D BP ecosystem.

In 2019 the 3D BP IC group published a background paper on communications, security, and privacy (CSP) [1], resulting in a focused effort by the 3D BP group to ensure these aspects were vetted, with the motivation and goal to bring together diverse stakeholders from technology, retail, research, and standards development to build thought leadership around 3D body processing technology standards in areas such as 3D capture, processing, storage, sharing, and (augmented) representation. The Communication, Security, and Privacy (CSP) subgroup focused on evaluating 3D scanning and processing technologies, identifying potential gaps in existing standards and recommending solutions for the IEEE P3141 Working Group. It also considered interoperability in terms of trustworthiness (i.e., communication, security, and privacy), identified and recommended deliverables (guidelines, practices, standards) for IEEE P3141 WG, and considered candidate use-case scenarios in terms of trusted 3D BP data.

The CSP subgroup engaged stakeholders in key areas (technologically and geographically) to get input that shaped the study. This engagement was in the form of a series of formal and informal discussions, which were augmented by input from university and industry researchers, as well as a review of workshop and conference papers. The structure of the CSP investigation included three principal areas: market, technology, and standards. After each of these three areas were examined, the role of academia and research as contributors to the three areas were considered. Finally, the importance of user acceptance was also addressed. There have been many bold predictions about where the exchange of high-fidelity 3D human body scans will eventually take various markets or sectors (e.g., apparel, fashion, health care, and automotive). However, there is no question that 3D body scanning is influencing consumers and impacting how people shop.

A key aspect of 3D BP is the intelligent connectivity of scanning technology and the resulting data, but the opportunity may be fragmented at this point. Early players are active and currently creating products for which they see a market. These players include various businesses and industries enabled by detailed anthropometric data, and they are implementing solutions, some of which may evolve into de facto standards, that may be creating an interoperability chasm. In order to get broader market acceptance, interoperability and trustworthiness are key considerations.

Founded as perhaps a niche application (e.g., airport security), 3D BP is now trending towards vertical

applications (consumer-goods, apparel, fashion, health care, automotive/transportation, and other industrial applications), with 3D BP development and deployment motivated by the desire to provide or enable customer experience and tailored needs (cheaper, faster, better), and by the desire to create new goods and services that will drive new revenue streams. Connecting 3D BP equipment and subsequent data transfers will open new markets, but at what costs to users? New products and business models will evolve and be disruptive with unintended consequences of technology deployment.

Improved communication and network technologies, along with the subsequent growth of personal data are further stressing privacy concerns. Consequently, the CSP examined technology needs and topics related to the expected disruptions in communications, security, and privacy.

The sections that follow highlight the discoveries and recommendations in the communications, security, and privacy aspects that the SCP subgroup proposes to the IEEE P3141 Working Group.

2. COMMUNICATIONS

The ability to connect to any device anywhere is essential to modern business. Being able to store and retrieve 3D body data with any personal device (such as smartphone, tablet, PC, thumb drive, or the cloud) saves time, reduces costs, and gives versatility to customers and retailers to manage items in the modern fashion industry.

With the increasing deployment of autonomous information systems, deep learning algorithms, and the growth of applications, data becomes an asset, as mined data can be transformed into meaningful information allowing individuals to be recognized by their behavior patterns. The CSP considers end-to-end privacy critical to the successful deployment of 3D BP solutions, and believes that it may be necessary to process data in such a manner to prevent intentional or unintentional release of personally identifiable information (PII), or any virtual representations (i.e., avatars).

Different devices require different connectivity options. One of the most popular options implemented on personal devices and peripherals include USB and wireless interfaces, such as IEEE Std 802.11, IEEE Std 802.15, and cellular communications, which provide a low cost, flexible interface for smart communications involving 3D body data.

IEEE P3141 will enable vendors and developers to use the aforementioned communication interfaces, offering customers and retailers a flexible modern implementation of 3D body processing.

3. MOTIVATIONS FOR PROVIDING SECURITY TO ENABLE TRUST IN AVATARS

The presence of entities in virtual worlds has increased in recent years, such that it is anticipated that perhaps 80% of internet users will have an avatar. The CSP group added Trust as this aspect is required for virtual worlds. This increase demonstrates the need for 3D BP diligence in terms of CSPT. As avatars may reflect personally identifiable information (PII) of real consumers (see Appendix A for PII definitions), there appears to be a need for the CSPT to address avatars to help ensure a shared understanding [2].

Avatars can range between high-fidelity statistical models or be generated from a focus population consisting of certain body shapes and measurements, or a model derived from a 3D point cloud of an individual. This range is identified in Table 1 as *Levels*. These levels are described in Section 5.3. Security and privacy must be preserved, regardless of the avatar fidelity level, unless the consumer or owner of the data specifically disables privacy protection.

Based on discussions related to data security and privacy, and other accumulated information, a preliminary matrix of the levels versus the trust components has been determined and is illustrated in Table 1. Avatar fidelity is a concern when the model is derived from a 2D point cloud of an individual, as well as the unintended consequences of data dissemination.

TABLE 1 Proposed avatar generation method versus trust components

Levels (fixed model—personal measurement model)	PII data (personal identifiable)	Communication	Security	Privacy Protection
Level 1 (common rough sizes)	No for avatar, yes when selling	Determine data owner	Low risk	No for avatar, yes when selling
Level 2 (adjustable model)	Yes	Data owner, data sharing, where is the data stored	Low to moderate risk	Yes
Level 3 Raw data point cloud (Avatar data + consumer id data)	Yes	Encrypt data	Moderate risk	Yes
Level 4 (Level 3 + fit preference towards products)	Yes	Encrypt data	Moderate to high risk	Yes
Level 5 (Level 4 + movement, soft body, etc.)	Yes	Encrypt data	High risk	Yes
Level 6 (e.g., perfect clone, face ID, body ID, PII, etc.)	Yes	Encrypt data	High risk	Yes

The details of the attributes are outside the scope of this paper but will be further refined as part of the formal WG effort in creating requirements in the standard.

3.1. REPRESENTATIVE IMPLEMENTATION OF USE CASE SCENARIOS

Select use-case scenarios are under development as points of consideration for the IEEE P3141 WG. They will be used in describing how data may be used. They show the possible stakeholders in a transaction, the types of transactions, and the outcomes produced by modifying a 3D Body Data package.

- UseCaseP3141-001-AvatarAugmentation
- UseCaseP3141-002-BodyScanUpdate

This top-level 3D Body Data block diagram, Figure 1, shows the basic content of a 3D BP file.

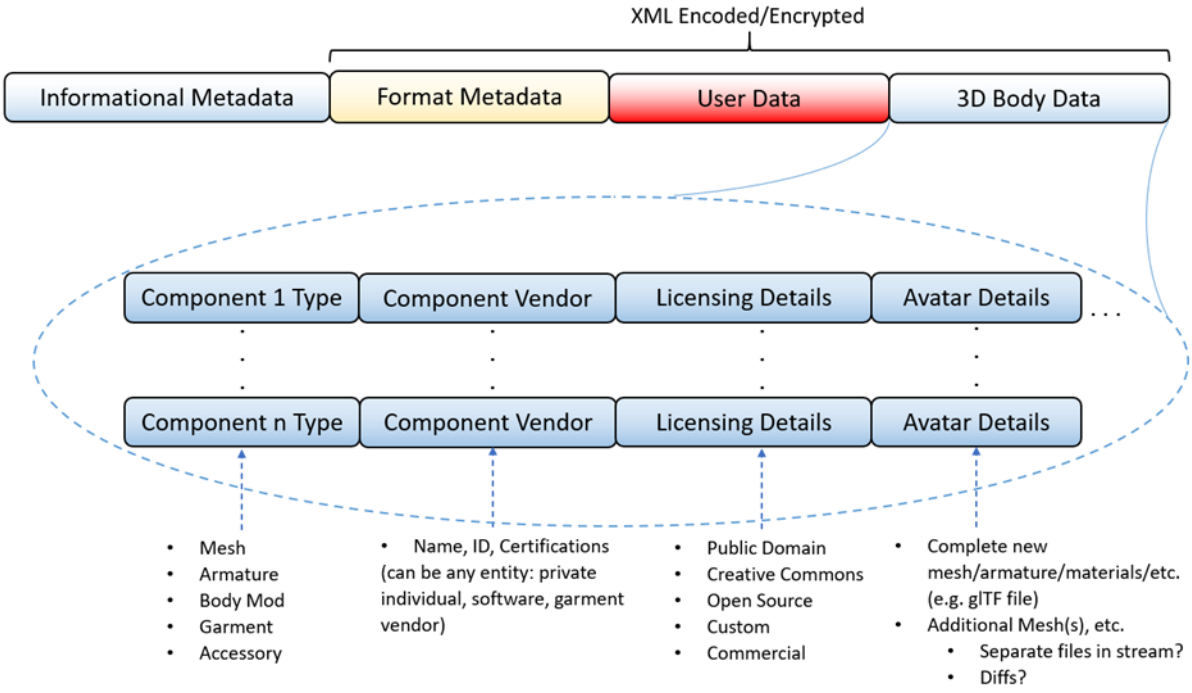

FIGURE 1 3D Body Data Block

3.2. FURTHER USE CASE INVESTIGATIONS

A number of areas for further Use Case development exist. These can be broken down by perspectives of various types of users. Examples include the following:

- Consumer's Perspective
  - Receive new 3D Body Data (body scan).
  - Purchase clothing based on 3D Body Data.
- Developer's Perspective
  - Design a body scanner with compliant output.
  - Develop a knitting machine to work with 3D Body Data input.
- Integrator's Perspective
  - Manage secured components of 3D Body Data.
  - Manage storage (local, cloud, etc.).
  - Create dynamic avatars based on body and clothing meshes.

4. SECURITY AND 3D BODY PROCESSING (3D BP)

3D human body processing is a many-sector, growing economic opportunity as part of a multi-billion-dollar business that includes medical, automotive, apparel and fashion, aerospace, pharmaceutical, art, sciences, and other sectors. However, existing 3D BP may have vulnerabilities that may impact security and privacy, or PII related matters. A secure framework for 3D BP can address the interaction of CSP in a trusted environment to help reduce vulnerabilities or identify mitigating solutions that enable trustworthiness of interoperability for users and stakeholders. It is recommended that the IEEE P3141 WG effort identify the details and approaches as outlined herein.

4.1. DEFINITIONS

3D Body Data Package: A (securely maintained) package of data containing a person's PII along with 3D body data used to make physical and virtual body-related purchases and other transactions.

avatar: In the context of 3D Body Processing, an avatar is a digital representation of the physical appearance of a user. There is a continuing conversation about naming 3D body scans as digital twins or digital clones. This paper operationalizes the term to be avatars. It is recommended for IEEE P3141 to further consider the details of this definition, and further define and refine to help ensure or prevent avatar ambiguity. That is, consideration must be given to the consumer who is unwilling or unable to have their full nude body scanned. In these cases, the avatar may be more completely represented in metadata rather than mesh data or the base mesh may start with the consumer approved scanning attire.

client (or consumer): The person/entity for which the 3D Body Processing Data package describes.

interoperability: A characteristic of a product or system, whose interfaces are compliant with IEEE P3141 to work with other tools in the data chain involved in this ecosystem.

presentation avatar: This is the avatar that a person wants to present for public view. This includes the nude base mesh (or other base mesh) with (applied body modifications, piercings, and clothing), rigging, and digital materials. Note that where fully scanned body mesh data is unavailable, some portion of the Presentation Avatar may need to be provided externally, and simply be "fitted" to the user's metadata where available.

user: The term "user" of data in this white paper refers largely to the entity who is taking the data as input. For each individual entity, that data may be used for either some final application (e.g., an avatar user) or as part of a chain of entity-driven operations (e.g., point cloud converted to landmark measurements by an apparel manufacturer).

vendor: An entity that has permission and the necessary keys to perform activity on the client's 3D Body Data package. The vendor may be an individual designer, a company, or a software package.

4.2. STATE-OF-THE-ART SECURITY

The IEEE P3141 focus on security and protection of data is a primary design criterion. Implementations lie on a technology platform that is conceived and designed to operate securely and is easy to manage.

The pillars of the security model include the following:

- Software security module to store and handle security information such as cryptographic keys, PIN codes, biometrics with full audit and log traces and secure key backup. The security module may perform cryptographic functions such as key management and authenticated encryption.
- Use of the Public Key Infrastructure (PKI) for issue and management of digital certificates for authentication and authorization of users and key management.
- Use of Elliptic Curve Cryptography (ECC) as well as the strongest cipher currently available such as block cipher AES or stream cipher Chacha20, both in authenticated mode as described in Section 4.3.
- Security management framework based on the NIST Cybersecurity Framework v 1.1.

4.3. INFORMATION SYSTEMS SECURITY

Information systems security comprises hardware, operating system, firmware, and application software collectively working to process and store data transformed into information for individuals and organizations. Information systems security includes the activities that secure and protect the information systems and the data on which the information systems operate.

NOTE—Currently, the consensus is that data may be a low-risk attribute, but with advancing techniques, the standard must consider the context of the data to help minimize vulnerability. That is, data is data, but once it is validated in context, the transformed data becomes information that must be protected.

4.3.1. 3D BP INFORMATION SYSTEMS

3D BP data may progress through multiple environments of Information Systems, each with a different degree of security and privacy. The lifecycle of 3D BP data begins with information systems capturing and processing sensitive data. The completed 3D BP data driven avatar may be provided to a production-based information system. The produced product, whether a garment or other item, will be delivered to the consumer. 3D BP information systems (3D BP) may be a mixture of information technology (IT), operational technology (OT), and 3D BP technology integrated with human interaction. The technology used depends on the point in the data lifecycle. The technology, whether IT or OT, is not the driver of security and privacy. Rather, the driver is the phase of the 3D BP data lifecycle.

4.3.1.1 DEVELOPMENT AND PROCESSING

Information systems used for the development, processing, and transmission work with sensitive data that requires security and privacy protection. The completed product should be anonymized when delivered to production information systems. All 3D BP data should be de-identified by the time it enters the production stage. The person's data (the body avatar but not PII that will link to a specific person) will be under an identification system that will be trackable.

4.3.1.2 PRODUCTION

The production 3D BP data without personal identifiers is business sensitive since identification is not uniquely tied to a specific person. The anonymization of data in the production stage, where OT is most likely, provides the

flexibility to leverage technology (not specifically designed for 3D BP) to be used without compromising security or privacy of the data. This approach also allows the sharing of production lines, which may be customizable for multiple product types or sources. Production-based information systems integrating intelligent systems and robotics are an implementation of cyber-physical social systems. These systems may include cyber-limited technology such as programmable logic controllers, and sensors limited in computational capacity that implement and operate cybersecurity controls. Cybersecurity control design must consider the computational ability to monitor and measure cybersecurity activity while maintaining scanning, storage, and delivery process performance. A balance between computational communications and the dynamics of the physical processes must be the foundation of well-defined cybersecurity control [3].

4.3.1.3 DELIVERED PRODUCT

The product will be de-anonymized post-production and will be tied back to the person since the product will need to be shipped to the person who requested it. Upon completion of production, the non-sensitive data would be tagged with an identification back to the person. The post-production 3D BP data is sensitive and will be protected by appropriate security and privacy controls. As such, the privacy guidelines are retained and maintained for future customer interaction.

4.3.2. CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY (CIA)

Information systems security is driven by the tenets of confidentiality, integrity, and availability. Confidentiality provides data that can only be viewed by authorized users. Confidentiality practices may include consideration of classification of the data and the implementation of protective technologies such as cryptography. Integrity allows for the change of information only by authorized users. Information will need to be maintained in a valid, uncorrupted, and accurate state. Availability provides access to the data by authorized users whenever they request the information. System availability refers to the time the system, applications, and data are available to and under control of authorized users. Availability may be measured in regard to uptime, downtime, mean-time-to-failure (MTTF), mean-time-to-repair (MTTR), and mean-time-between-failures (MTBF). Restoration of unavailable systems may be measured in recovery time objective (RTO) and recovery point objective (RPO). 3D BP data, once processed, is completely electronic and logically stored. The processed 3D BP data may be protected with classical on-premises backup methods, as well as backups in the cloud. Backup controls should comply with security and privacy requirements based on the life-cycle stage of the 3D BP data.

4.3.3. IMPLICATIONS OF 3D BP AND CIA

The breach of data or compromise of a 3D BP information system has implications of safety, security, and other impacts. These incidents are defined by several risk factors as outlined in NIST SP 800-63 [4], Section 6.2. The risk factors include the following:

1) Potential impact of inconvenience, distress, or damage to standing or reputation
2) Financial loss or institutional liability
3) Harm to institution programs or public interests
4) Unauthorized release of sensitive information (any PII)
5) Personal safety
6) Civil or criminal violations

4.3.4. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

3D BP developers, implementers, and user organizations are responsible for maintaining security of the 3D BP information systems and data therein. 3D BP Organizations should follow information security management systems as provided in ISO/IEC 27002 [5]. ISO/IEC 27002 is within the context of the confidentiality, integrity, and availability (CIA) triad. The standard includes the following:

- Structure
- Security Policy
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- Information Systems Acquisition, Development, Maintenance
- Supplier Relationships
- Information Security Incident management
- Information Security Aspects of Business Continuity
- Compliance

4.4. 3D BP INFORMATION DATA MODEL

The 3D BP data model is an integration of diverse data involved in the capture, classification, storage, and transmission of data ultimately describing a 3D Body (see Figure 1). Data classification varies as well as licensing, which ranges from private to the public domain. 3D BP data when not being actively processed may be at rest or in transit. The data may be shared external to the developer, implementer, and user organization via wired and wireless interfaces and cellular-based protocols. Organizations will need to make careful consideration of the risk of confidentiality and integrity breaches during data processing, as well as 3D BP data at rest or in transit. Given the nature of the 3D BP collaborative environments, numerous connectivity methods, and limited processing power of some components, organizations will need to weight the type of cryptography implemented at each data state. Additional measures may be considered to avoid inference issues when transferring anonymized data. The goal of cryptography is to provide for confidentiality, integrity, authentication, and nonrepudiation. Organizations developing, processing, transmitting, or producing 3D BP data should implement an information security encryption algorithm, such as ISO/IEC 18033 series of standards specifying “encryption systems (ciphers) for the purpose of data confidentiality” [6]. Depending on geographic and government laws, 3D BP organizations may be subject to local regulations or standards such as NIST SP 800-175B [7] as a guideline for cryptographic standards.

4.5. 3D BP SECURITY EVALUATION

A 3D BP network may be confined to a set of components capturing and integrating 3D measurements, as well as interconnecting to internal, external, and cloud computing components. 3D BP technologies from a network viewpoint may exist in all layers of the Open Systems Interconnection Model (OSI). 3D BP connections may include wired and wireless transmissions and cellular-based protocols. 3D BP data processing occurs in the application layer. Encryption of data in transit happens between the application layer and the transport layer. Depending on the life-cycle stage and implemented technology appropriate controls for that life-cycle stage and OSI layer should be implemented to meet security and privacy requirements.

Each organization will be able to define a 3D BP Trusted Computing Base (TCB). The TCB includes the hardware, software, and firmware critical to the security of the 3D BP information system. Any vulnerabilities inside the TCB, given exposure and threat agents, may lead to compromise. 3D BP organizations should design the systems with security principles and processes towards data leak prevention and testability. Agents external to the TCB should not be able to cause a data leak or gain privilege escalation other than granted by policy and design. The development will lead towards the definition of a security perimeter defining the boundary of the TCB and a reference monitor mediating requests and allowing access to authorized subjects. 3D BP organizations should establish functional and assurance requirements and test those requirements in accordance with ISO/IEC 15408-1 [8].

4.6. RISK MANAGEMENT

A risk management program includes risk assessment, risk mitigation, and evaluation and assurance. Risk assessment includes the identification of risk, evaluation of risks and risk impact, and the recommendation of risk reducing measures. Risk reducing efforts include risk avoidance, risk mitigation, risk acceptance, and risk transference. The risk management process is an ongoing process with periodic evaluations, assessments, and regulatory compliance. 3D BP organizations will be subject to laws, regulations, and compliances varying with geographic operational areas. Some compliance requirements may be global such as the PCI Data Security Standard (PCI-DSS) [9] or General Data Protection Regulation (GPDR) . Other compliance requirements may be more localized, such as Cybersecurity Maturity Model Certification (CMMC) , Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (NIST SP 800-171 [12]) , and Health Insurance Portability and Accountability Act (HIPAA) [13]. Compliance identification and assessments are part of a risk management program. 3D BP organizations may consider ISO/IEC 31000 [14] as applicable to their organization. 3D BP organizations should implement a risk management process, as defined in ISO/IEC 27005 [15]. ISO/IEC 27005 describes risk from the viewpoint of information security. The standard includes examples of approaches to information security risk assessments. ISO/IEC also details possible threats, vulnerabilities, and security controls that may be encountered or implemented.

5. AVATAR DESIGN

5.1. CONSIDERATIONS FOR AVATAR USERS

Supporting the public presentation of a personal avatar (e.g., in the metaverse) is an important role of the 3D Body Data package owned by each person. To this end, the data package must allow for augmentations (either destructive or non-destructive) to be applied to the original body data for presentation purposes. One example of

this is the addition of clothing to a garmentless or appropriate scanning garment base mesh obtained from a 3D body scanner. This modification may very well be done by a clothing vendor at the time of purchase of a physical piece of apparel.

The modifications may be done destructively by directly editing the existing body mesh to include the clothing. This is generally more performant for avatar presentation but will affect a loss of measurement accuracy in key body areas (depending on the modification). One would not be able to use a presentation avatar for body measurement purposes.

The modifications may also be done non-destructively, whereby new meshes are added to the 3D Body Data package as completely separate components. This brings some level of immunity of body measurement accuracy at the expense of complexity and poor avatar performance during presentation.

5.2. CONSIDERATIONS FOR AVATAR VENDORS

Different levels of "exclusivity" can exist among different vendors of avatar content. Vendors ranging up and down the magnitude scale (from individual developers to full media companies) can be involved in this same "mesh-creating" process, and some vendors are more concerned about their rights to their content than others.

Most of the larger vendors may have the resources to maintain custom licenses for their content, while the smaller individual contributors will likely choose from the available free and open-source licenses. The following are the most common free licenses currently used by individual 3D content creators.

Creative Commons (simple and well drafted licenses)

(https://creativecommons.org/licenses/)

- Public Domain (CCO)
- Attribution (CC BY)
- Attribution ShareAlike (CC BY-SA)
- Attribution-nonDerivs (CC BY-ND)
- Attribution-Noncommercial (CC BY-NC)
- Attribution-Noncommercial-ShareAlike (CC BY-NC-ND)
- Attribution-Noncommercial-NonDerivs (CC BY-NC-ND)

Open Source (mostly used for software but is also used for assets as well).

All of these licenses provide Attribution, Open Source, and Non-Liability clauses.

1) MIT (https://opensource.org/licenses/MIT)
2) BSD (https://opensource.org/licenses/BSD-3-Clause)
3) Apache (https://www.apache.org/licenses/LICENSE-2.0)

Further, a content vendor may be under contract to yet another vendor that may have provided them with the base content or tools used to augment a client's avatar.

Still, even with all these considerations and options, licenses are not magic. They do not enforce themselves. This is where the need for security in avatar handling is currently most needed by content creators. That is to say, this makes “avatar security” somewhat separate from the more pressing considerations of PII security.

A goal here is to allow for controlled “cross-talk” between vendors and their products (as may or may not be allowed). For example, Pants vendor A may not want Shirt vendor B to be able to modify the pants when the client purchases a new shirt. However, it may be perfectly desirable and legal for the client to hire artist C to place the client’s logo on their pants.

Ensuring the secure transfer of information at each stage of the 3D BP chain is instrumental to the overall security required by the end user (the person whose identity is being protecting). The components in this processing chain will likely change over time as technology advances and as new applications arise. To allow flexibility in selection of future process components, security must be applied at each processing stage, as well as the realization that secure data transfer will likely take place across a number of separate stages, all of which need to apply security and handle their part in a secure manner.

5.3. ON THE FIDELITY LEVEL OF AVATARS

Different fidelity levels help to identify the suitability of an avatar for use in a specific application. Some applications may be considered more “critical” where, for example, a measurement is to be taken for purchasing a piece of clothing. But other applications may require less stringent specifications where simple public rendering may be sufficient.

From a high viewpoint, avatar fidelity refers to its usability in some specified class of activity. For example, with respect to the apparel industry, the following list is representative of increasing fidelity levels that might be used to describe a type of clothing purchase. Avatar fidelity can range from fixed dimension (i.e., ready to wear) dimension to accurate, high-quality levels. The IEEE P3141 WG will further refine these details and provide descriptions to ensure a reasonable level of privacy and security can be provided.

Raw:

- Accurate reproduction of critical body measurements from raw point/mesh data.
- Accurate body measurement metadata (including quality data).

Cosmetic:

- Renderable nude body mesh or approved scanning attire body mesh (including rigging, materials, etc.).
- Renderable full body mesh (including clothes, jewelry, etc.).
- Separable mesh modifications (clothes, jewelry, etc.).
- Variable fidelity content (low poly render).

5.4. AVATAR FIDELITY IN APPAREL, FOOTWEAR, AND WEARABLES INDUSTRIES

In considering the principles of ergonomics and anthropometry in the apparel/footwear/wearables industries, the complexity and diversity of body shapes makes the notion of perfectly fitting clothing, footwear, or wearables extremely challenging. With advancement of technology, body scans enable data extraction and synthesis, and avatars may be the next step in fashion and apparel. Data extraction can range from 1D measurements, 2D measurements with location and orientation, to full 3D measurements and 3D body shape and surface understanding. Avatar Fidelity Level is an effort to explore the suitability of the 3D Body Data to be applied during a given application that may reside on a person's mobile device (i.e., cellphone). Avatar Fidelity Level may have a number of dimensions to consider.

6. PRIVACY

Privacy is a sophisticated concept, and its definition may vary depending on individual backgrounds, past experiences, cultures or societal norms, or prevailing political/societal environments. As stated in IEEE Std 802E-2020, "The term Privacy was used in many contexts and is defined in multiple ways." (p.14). Therefore, the CSPT group recommends defining privacy protection as preventing disclosure of users' information such as, username, ID, preferences, and user history, etc., to unauthorized parties, third party interconnections, or those not specified explicitly by the user.

In the context of 3D body scanning, the CSPT subgroup has identified the following potential privacy considerations/treats that warrant a closer examination for establishing IEEE P3141. For instance, the yearbook photo scenario (or an old driver's license photo) may provide an analog for expired data—the data were valid at a certain time point but may not be valid on reflecting a real-time reality after a certain period of time. Depending on the user scenarios, companies may consider design mechanisms that ask for or remind/request for data updates/authorization, or have a subject authorize the use of their body scanning data to ensure the data accuracy and validity.

In addition to the GDPR that was passed on May 25, 2018, the California Consumer Privacy Act (CCPA) [16] came into effect on January 1st, 2020. Enforcement began July 1st, 2020. Other US states have passed privacy acts. This paper will not be reviewing any others.

6.1. CCPA—CALIFORNIA CONSUMER PRIVACY ACT

In 2018, California passed the CCPA to become the first US state that has a comprehensive consumer privacy law. In this section, the goals of the CCPA and some differences between CCPA and GDPR will be discussed. GDPR was meant to protect EU residents' privacy; whereas CCPA grants some new rights to the residents of California regarding their personal information and requires certain entities to fulfill various data protection duties. Specifically, CCPA covers the following four rights:

1) The right to know about the personal information a business collects and how it is used and shared;
2) The right to delete personal information collected (with some exceptions);

3) The right to opt-out of the sale of their personal information; and

4) The right to non-discrimination for exercising their CCPA rights.

The CCPA defines personal information as follows: “It includes any information that directly or indirectly identifies, describes, relates to, is capable of being associated with, or can reasonably link to a particular consumer or household. The statutory definition includes eleven specific categories that businesses must use when providing their required disclosures” (p. 8).

Any for-profit entity that operates a business in California would need to comply with CCPA if they

- Generate more than $25 million gross revenue, or
- Collect more than 50,000 consumers, households, or devices for commercial purposes, or
- Make more than 50% of the annual revenue from selling consumer data.

Under CCPA, the definitions of consumers include customers of goods or services, employees, and business-to-business transactions. Therefore, like GDPR, they both have potential extraterritorial effects on entities that operate or reside outside of jurisdictional territory (i.e., state of California or EU).

Like GDPR, CCPA protects personal information relating to an identified data subject or identifiable personal data subject. However, CCPA also includes information linked at the household or device level. Note that certain information is not protected if included in publicly-available government records such as government, financial records, social media, or if covered by specific legislation.

6.1.1. DE-IDENTIFIED PERSONAL DATA

CCPA does not forbid a business to disclose or sell consumer information if it is de-identified or aggregated. However, it is the company's responsibility to show the data is de-identified or aggregated. In GDPR, the pseudonymous data is considered personal data and CCPA has a similar definition on pseudonymization. Both require technical controls for re-identification to qualify for claiming pseudonymous data.

6.1.2. PRIVACY NOTICE—RIGHT TO KNOW

In terms of the privacy notice, CCPA requires companies to inform consumers what personal information categories are collected and their intended use for each category. If a company decides to collect additional personal information categories or use the collected personal information for unrelated purposes, a follow-up notice will be required. If a third-party company is involved, consumers should be provided with explicit notice and given a choice to opt-out before reselling consumers’ personal data.

6.1.3. OPT-OUT RIGHT FOR SELLING PERSONAL INFORMATION

CCPA requires companies to include “Do Not Sell My Personal Information” link on a company’s website homepage. Once a consumer chooses opt-out, the company should not request reauthorization to sell the data within 12 months of the opt-out request. GDPR does not use “do not sell my data;” however, a data subject may withdraw consent for processing activities at any time to opt-out of a third-party data sell. Similar to GDPR, CCPA also allows Right of Disclosure or Access, which means that California consumers can obtain a written disclosure of their personal information and what data category the business collects on them, the use purposes, and if the data were shared with any third parties [17].

6.1.4. NON-DISCRIMINATION FOR EXERCISING CCPA RIGHTS

CCPA asks companies to refrain from discriminating against consumers if they exercise their rights. However, CCPA allows companies to provide financial incentives to encourage consumers' opt-in for data sharing; and companies can charge more if the price increase can be rationalized by the value of consumer's data.

In contrast with GDPR, CCPA did not regulate the following rights:

- Right of Rectification
- Right to Restrict Processing
- Right to Object to Processing

Regarding the penalty of a violation, GDPR fines can reach 20 million EUR or 4% of annual global revenue, whichever is higher. For CCPA, The California Attorney General may bring civil penalties of $2500 per violation or up to $7500 per violation if intentional.

6.2. APEC PRIVACY FRAMEWORK

In the Asia-Pacific region, there is an APEC privacy framework published by the Asia-Pacific Economic Cooperation in 2015 [18]. The framework aims to facilitate regional transfers of personal information while protecting individual privacy within and beyond political jurisdictions.

The principles of APEC privacy framework include the following:

1) Preventing Harms
2) Notice
3) Collection Limitation:
4) Uses of Personal Information
5) Choice
6) Integrity of Personal Information
7) Security Safeguards
8) Access and Correction
9) Accountability

Currently in the United States, there is no comprehensive data protection law as in the EU. However, under CCPA, any inferences (such as preferences, behaviors, and characteristics) drawn from consumers' personal information are also defined as personal data. There is a possibility that 3D body scanning data can be used to obtain information on health or wellness and potential health risks, which in turn, may lead to discrimination on insurance premium charges. The World Economic Forum published a briefing paper addressing the similar concerns on the potential risks of discriminations involved with data-drive inferences using the Internet of Bodies data [19]. It is recommended that IEEE P3141 WG further consider these documents when developing the standard.

6.3. DIFFERENTIAL PRIVACY

Differential privacy (DP), homomorphic encryption (HE), and secure multi-party computation (SMPC) are components of an evolving privacy-enhancing method designed for computational analysis that may be used in 3D BP, as components to address 3D BP privacy-related matters.

Differential privacy is tailored to the problem of statistical disclosure control such that publicly released statistical information about a set of people does not compromise the privacy of any individual. Differential privacy requires that the probability distribution on the statistical analysis of published results is "essentially the same," independent of whether any individual opts in to, or opts out of, the data set. Statistical databases are typically created to achieve a social goal, such that increased participation in the databases improves the likelihood analysis. Thus, differential privacy can further enable a social goal by ensuring privacy preservation of each individual, such that they incur lower risk by joining the database. Key attributes of differential privacy include a privacy framework that is independent of any additional information, including other databases, available to an adversary, such that privacy is realizable using simple and general mechanisms, and it permits accurate analysis as the database grows.

Differential privacy data analysis is focused on the setting of a trusted curator holding a large, static, data set, and permanent storage in a tamper proof system. The curator either responds to queries (the interactive case) or prepares some sort of summary or synthetic database (the non-interactive case), intended to answer all queries of a particular type.

HE is an encryption technique that allows computation to be performed directly on encrypted data and anonymized datasets. The computation occurs without losing context of the data and may be an enabler for 3D BP security and privacy-preservation.

SMPC is part of cryptology intended for parties to jointly work on computations while preserving inputs as private data.

The 3D BP CSPT recommends that the IEEE P3141 WG further investigate these technologies as perhaps niche solutions that further enable the deployment of 3D BP.

7. CONCLUSION AND RECOMMENDATIONS

3D BP metadata may allow or enable the unintended disclosure of the identity of an individual, or at least of the individual's preferences and behavior (PII). The current lack of dissociable engineering solutions has led to a proliferation of this type of disclosure of individual identity. In this realm, it is also vital that devices and applications cease to share information covertly without user consent. Current applications may intentionally or unknowingly share data or respond to request for data access. Wireless devices transmitting non-user specific telemetry can create privacy risks for individuals. It is essential that the predictability principle consider both users created data and device/software metadata. There are ongoing standards efforts by the IEEE Standards Association, such as IEEE P7002 and IEEE P1912, and it appears these standards will be complimentary components to IEEE P3141 and may be leveraged as normative or informative content to help address autonomous information systems or edge-related technologies, in terms of privacy, as it relates to 3D BP and the development of IEEE P3141.

8. REFERENCES

The following list of sources either has been referenced within this paper or may be useful for additional reading:

[1] IEEE 3D Body Processing Industry Connections (3D BP IC): Communication, Security, and Privacy, 2019 3D BP CSP White Paper, https://standards.ieee.org/content/dam/ieee-standards/standards/web/governance/iccom/3DBP-Communication_Security_Privacy.pdf.

[2] Fred Miao, Irina Kozlenkova, Haizhong Wang, Tao Xie, and Robert Palmatier, An Emerging Theory of Avatar Marketing," Journal of Marketing. https://doi.org/10.1177/0022242921996646.

[3] Sachin Sen and Paul Pang. Architectural Modeling and Cybersecurity Analysis of Cyber-Physical. International Research Journal of Engineering and Technology. DEC 2018; 5(12):1107. https://doi.org/10.3390/s18051643.

[4] NIST SP 800-63 Revision 3, Digital Identity Guidelines, https://doi.org/10.6028/NIST.SP.800-63-3.

[5] ISO/IEC 27002, Information technology—Security techniques—Code of practice for information security controls.

[6] ISO/IEC DIS 18033-1, Information security—Encryption algorithms—Part 1: General.

[7] NIST SP 800-175B Revision 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.

[8] ISO/IEC 15408-1, Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model.

[9] Payment Card Industry (PCI) Data Security Standard, Version 3.2.1, PIC Security Standards, Council, LLC, Wakefield, MA USA, MAY 2018.

[10] European Parliament and of the Council, Strasbourg, (2016, Apr. 27), General Data Protection Regulation, Regulation (EU) 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[11] Cybersecurity Maturity Model Certification (CMMC), Version 1.02, Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory, Pittsburgh, PA, USA and Laurel, MS, USA, MAR 2018.

[12] NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

[13] House of Representatives 104th Congress 2d Session (1996, Jul. 31), Health Insurance Portability and Accountability Act of 1996, H. Rept. 104-736, https://www.govinfo.gov/app/details/CRPT-104hrpt736/CRPT-104hrpt736.

[14] ISO/IEC 31000, Risk Management—Guidelines.

[15] ISO/IEC 27005, Information technology—Security techniques—Information security risk management.

[16] California State Legislature (2018), California Consumer Privacy Act of 2018, TITLE 1.81.5 m https://oag.ca.gov/privacy/ccpa.

[17] Laura Jehl & Alan Friel, CCPA and GDPR Comparison Chart, https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.

[18] APEC Privacy Framework, Asia-Pacific Economic Cooperation, Singapore, 2015, https://iapp.org/resources/article/apec-privacy-framework/.

[19] Liu, X., & Merritt, J. (2020). Shaping the Future of the Internet of Bodies: New challenges of technology governance. http://www3.weforum.org/docs/WEF_IoB_briefing_paper_2020.pdf.

9. APPENDIX A PERSONALLY IDENTIFIABLE INFORMATION

Personally Identifiable Information is defined by IEEE Std 802E™-2020, ISO/IEC 27018-2019, and NSIT SP 800-79-2 as follows:

- IEEE Std 802E-2020, IEEE Recommended Practice for Privacy Considerations for IEEE 802®Technologies.

  Personally Identifiable information (PII) is defined as any data that can be reasonably linked to an individual based on their unique physical, digital, or virtual identity.

- ISO/IEC 27018:2019, Information technology—Security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

  PII: Any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person. Note 1 to entry: The “natural person” in the definition is the PII principal (3.4).

- NIST SP 800-79-2, Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI).

  Personally Identifiable Information: Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571